506P037OUS00 #1

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ３月１４日

出 願 番 号
Application Number: 特願２０００－０６９６９７

出 願 人
Applicant (s): ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年１２月２２日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２０００－３１０６１３７

【書類名】　特許願

【整理番号】　9900878406

【提出日】　平成12年 3月14日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 12/16

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　郷　直美

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　栗原　章

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100082131

【弁理士】

【氏名又は名称】　稲本　義雄

【電話番号】　03-3369-6479

【手数料の表示】

【予納台帳番号】　032089

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9708842

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　情報提供装置および方法、情報処理装置および方法、並びにプログラム格納媒体

【特許請求の範囲】

【請求項１】　第１の情報処理装置を認証する第１の認証手段と、

第２の情報処理装置を認証する第２の認証手段と、

前記第１の情報処理装置からの、前記第２の情報処理装置を特定するデータおよび鍵の送信要求の受信を制御する受信制御手段と、

前記第２の情報処理装置を特定する前記データに基づき、前記第２の情報処理装置に前記鍵の送信要求を送信するとともに、前記第２の情報処理装置から前記鍵を受信するように通信を制御する通信制御手段と、

前記第１の情報処理装置への前記鍵の送信を制御する送信制御手段と

を含むことを特徴とする情報提供装置。

【請求項２】　第１の情報処理装置を認証する第１の認証ステップと、

第２の情報処理装置を認証する第２の認証ステップと、

前記第１の情報処理装置からの、前記第２の情報処理装置を特定するデータおよび鍵の送信要求の受信を制御する受信制御ステップと、

前記第２の情報処理装置を特定する前記データに基づき、前記第２の情報処理装置に前記鍵の送信要求を送信するとともに、前記第２の情報処理装置から前記鍵を受信するように通信を制御する通信制御ステップと、

前記第１の情報処理装置への前記鍵の送信を制御する送信制御ステップと

を含むことを特徴とする情報提供方法。

【請求項３】　第１の情報処理装置を認証する第１の認証ステップと、

第２の情報処理装置を認証する第２の認証ステップと、

前記第１の情報処理装置からの、前記第２の情報処理装置を特定するデータおよび鍵の送信要求の受信を制御する受信制御ステップと、

前記第２の情報処理装置を特定する前記データに基づき、前記第２の情報処理装置に前記鍵の送信要求を送信するとともに、前記第２の情報処理装置から前記鍵を受信するように通信を制御する通信制御ステップと、

前記第１の情報処理装置への前記鍵の送信を制御する送信制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【請求項４】　第１の情報提供装置を認証する認証手段と、

前記第１の情報提供装置への、鍵を提供する第２の情報提供装置を特定するデータおよび前記鍵の送信要求の送信を制御する送信制御手段と、

前記第２の情報提供装置から前記第１の情報提供装置が提供を受け、送信した前記鍵の受信を制御する受信制御手段と

を含むことを特徴とする情報処理装置。

【請求項５】　第１の情報提供装置を認証する認証ステップと、

前記第１の情報提供装置への、鍵を提供する第２の情報提供装置を特定するデータおよび前記鍵の送信要求の送信を制御する送信制御ステップと、

前記第２の情報提供装置から前記第１の情報提供装置が提供を受け、送信した前記鍵の受信を制御する受信制御ステップと

を含むことを特徴とする情報処理方法。

【請求項６】　第１の情報提供装置を認証する認証ステップと、

前記第１の情報提供装置への、鍵を提供する第２の情報提供装置を特定するデータおよび前記鍵の送信要求の送信を制御する送信制御ステップと、

前記第２の情報提供装置から前記第１の情報提供装置が提供を受け、送信した前記鍵の受信を制御する受信制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報提供装置および方法、情報処理装置および方法、並びにプログラム格納媒体に関し、特に、コンテンツを復号する鍵を提供するか、または暗号化されているコンテンツを利用する情報提供装置および方法、情報処理装置および方法、並びにプログラム格納媒体に関する。

【０００２】

【従来の技術】

図１は、従来のデジタルデータ伝送システムの構成を示す図である。パーソナルコンピュータ１は、ローカルエリアネットワークまたはインターネットなどから構成される通信ネットワーク４に接続されている。パーソナルコンピュータ１は、コンテンツサーバ２２から受信した、またはCD（Compact Disc）から読み取った楽音のデータ（以下、コンテンツと称する）を、所定の圧縮の方式（例えば、ATRAC3（商標））に変換するとともにDES（Data Encryption Standard）などの暗号化方式で暗号化して記録する。

【０００３】

パーソナルコンピュータ１は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

【０００４】

利用条件のデータは、例えば、その利用条件のデータに対応するコンテンツを同時に利用することができるポータブルデバイス（Portable Device（PDとも称する））の台数（後述する、いわゆるチェックアウトできるPDの台数）を示す。利用条件のデータに示される数だけコンテンツをチェックアウトしたときでも、パーソナルコンピュータ１は、そのコンテンツを再生できる。

【０００５】

パーソナルコンピュータ１の表示操作指示プログラム１１は、パーソナルコンピュータ１が記録しているコンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、チェックアウトの指示などを入力して、ＳＤＭＩ（Secure Digital Music Initiative）の規格に準拠したソフトウェアモジュールであるＬＣＭ（Licensed Compliant Module）１２にその指示に対応したチェックアウトなどの処理を実行させる。

【０００６】

パーソナルコンピュータ１のＬＣＭ１２は、コンテンツの不正な２次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から

構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

【０００７】

ＬＣＭ１２は、パーソナルコンピュータ１に接続された機器が正当であるかの認証を行い、安全な方法でコンテンツの移動の処理などを実行する。コンテンツの移動の処理などに伴い、ＬＣＭ１２は、必要な鍵を生成して、鍵を管理し、コンテンツを暗号化し、または接続されている機器との通信を制御する。

【０００８】

また、ＬＣＭ１２は、装着されているポータブルメディア３の正当性をチェックして、サーバ５が指定した利用条件をコンテンツ（暗号化されている）に付加して、コンテンツを記録させる。

【０００９】

パーソナルコンピュータ１のＬＣＭ１２は、暗号化して記録しているコンテンツを、コンテンツに関連するデータ（例えば、曲名、または利用条件など）と共に、接続されているポータブルデバイス２に供給するとともに、ポータブルデバイス２に供給したことに対応して、供給したコンテンツに対応する利用条件のデータを更新する（以下、チェックアウトと称する）。より詳細には、チェックアウトしたとき、パーソナルコンピュータ１が記録している、そのコンテンツに対応する利用条件のデータのチェックアウトできる回数は、１減らされる。チェックアウトできる回数が０のとき、対応するコンテンツは、チェックアウトすることができない。

【００１０】

ポータブルデバイス２は、パーソナルコンピュータ１から供給されたコンテンツ（すなわち、チェックアウトされたコンテンツ）を、コンテンツに関連するデータ（例えば、曲名、または利用条件など）と共に、装着されているポータブルメディア３に記憶させる。

【００１１】

ポータブルメディア３は、フラッシュメモリなどの記憶媒体をその内部に有し、ポータブルデバイス２に着脱可能に構成されている。

【００１２】

ポータブルデバイス２は、コンテンツに関連する利用条件のデータに基づいて、装着されているポータブルメディア３に記憶されているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。

【００１３】

例えば、コンテンツに関連する利用条件のデータとして記憶されている、再生制限としての再生回数を超えて再生しようとしたとき、ポータブルデバイス２は、対応するコンテンツの再生を停止する。

【００１４】

使用者は、コンテンツを記憶したポータブルデバイス２をパーソナルコンピュータ１から取り外して、持ち歩き、ポータブルメディア３に記憶されているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【００１５】

ポータブルデバイス２がUSBケーブル等を介してパーソナルコンピュータ１に接続されたとき、ポータブルデバイス２とパーソナルコンピュータ１とは、相互認証の処理を実行する。この相互認証の処理は、チャレンジレスポンス方式の認証の処理である。チャレンジレスポンス方式とは、パーソナルコンピュータ１が生成するある値（チャレンジ）に対して、ポータブルデバイス２がパーソナルコンピュータ１と共有している秘密鍵を使用して生成した値（レスポンス）で応答する方式である。

【００１６】

サーバ５は、所定の方式で圧縮符号化され、暗号化されたコンテンツを蓄積して、パーソナルコンピュータ１からの要求に対応して蓄積しているコンテンツを配信する。サーバ５は、鍵サーバ２１、コンテンツサーバ２２、およびショップサーバ２３の機能を有する。

【００１７】

鍵サーバ２１は、コンテンツサーバ２２がパーソナルコンピュータ１に供給したコンテンツを復号するためのコンテンツ鍵を蓄積し、パーソナルコンピュータ

１の要求に対応して、コンテンツ鍵をパーソナルコンピュータ１に供給する。コンテンツ鍵の供給の前に、鍵サーバ２１とパーソナルコンピュータ１とは、相互認証の処理を実行して、鍵サーバ２１は、その相互認証の処理により共有された一時鍵でコンテンツ鍵を暗号化して、パーソナルコンピュータ１に送信する。パーソナルコンピュータ１は、受信したコンテンツ鍵を共有している一時鍵で復号する。

【００１８】

コンテンツサーバ２２は、パーソナルコンピュータ１の要求に対応して、通信ネットワーク４を介して、パーソナルコンピュータ１に、コンテンツに対応する利用条件と共にコンテンツ（暗号化されている）を供給する。

【００１９】

ショップサーバ２３は、コンテンツサーバ２２が供給するコンテンツに関連するデジタルデータ（コンテンツの曲名、価格などを含むコンテンツの一覧などを含む）をパーソナルコンピュータ１に提供するとともに、パーソナルコンピュータ１からのコンテンツの購入の申し込みに対応して、そのコンテンツを供給するコンテンツサーバ２２のＵＲＬ（Uniform Resource Locator）、およびそのコンテンツを復号するコンテンツ鍵を供給する鍵サーバ２１のＵＲＬなどをパーソナルコンピュータ１に供給する。

【００２０】

次に、図２を参照して、従来のデジタルデータ伝送システムの機能の構成について説明する。パーソナルコンピュータ１は、表示操作指示プログラム１１およびＬＣＭ１２に加えて、ＩＰ（Internet Protocol）通信プログラム１３、ＩＳＰ（Internet Service Provider）接続プログラム１４、およびＰＨＳ（Personal Handyphone System）／ＩＭＴ（International Mobile Telecommunication System）通信プログラム１５を実行する。

【００２１】

ＰＨＳ／ＩＭＴ通信プログラム１５は、公衆回線網３１を介して通信を行うためのプログラムである。ＩＳＰ接続プログラム１４は、ＩＳＰ３２と接続するためのプログラムである。ＩＰ通信プログラム１３は、ＨＴＴＰ（Hypertext Tran

sport Protocol）７１およびＷａｐ（Wireless Access Protocol）７２などの手続を包含し、通信ネットワーク４を介して、鍵サーバ２１、コンテンツサーバ２２、またはショップサーバ２３と通信するためのプログラムである。

【００２２】

ＬＣＭ１２は、ライセンス管理プログラム５１、鍵管理プログラム５２、コンテンツ管理プログラム５３、鍵情報受信プログラム５４、およびコンテンツ情報受信プログラム５５から構成されている。

【００２３】

ライセンス管理プログラム５１は、コンテンツの利用条件に基づいたコンテンツの利用を管理するためのプログラムであり、利用条件管理プログラム６１、CDリッピングプログラム６２、コンバータプログラム６３、およびPD認証プログラム６４から構成されている。

【００２４】

利用条件管理プログラム６１は、コンテンツの利用条件に基づいて、パーソナルコンピュータ１が記録しているコンテンツのチェックアウトなどを許可するか、または禁止するかなどの管理を実行するとともに、コンテンツのチェックアウトなどに対応して利用条件のデータを更新する。CDリッピングプログラム６２は、パーソナルコンピュータ１に装着されたCDからコンテンツを読み出すとともに、読み出したコンテンツに対応する利用条件を生成する。

【００２５】

コンバータプログラム６３は、コンテンツの暗号化方式、または符号化方式を変換する。PD認証プログラム６４は、パーソナルコンピュータ１に装着されているポータブルデバイス２を認証する。

【００２６】

鍵管理プログラム５２は、鍵サーバ２１の認証の処理を実行して、鍵サーバ２１からコンテンツ鍵を受信して、コンテンツに対応させてコンテンツ鍵を管理する。鍵管理プログラム５２は、サーバ認証プログラム６５および受信プログラム６６から構成される。

【００２７】

サーバ認証プログラム６５は、後述する処理により、鍵サーバ２１を認証する。受信プログラム６６は、通信ネットワーク４を介して、鍵サーバ２１からコンテンツ鍵を受信する。

【００２８】

コンテンツ管理プログラム５３は、通信ネットワーク４を介して、コンテンツサーバ２２からコンテンツの利用条件のデータとともにコンテンツを受信して、コンテンツの利用条件のデータとともにコンテンツを記録する。コンテンツ管理プログラム５３の受信プログラム６７は、コンテンツサーバ２２からコンテンツの利用条件のデータおよびコンテンツを受信する。

【００２９】

鍵情報受信プログラム５４は、ショップサーバ２３から、所望のコンテンツに対応するコンテンツ鍵を供給する鍵サーバ２１を特定するＵＲＬを受信する。コンテンツ情報受信プログラム５５は、ショップサーバ２３から、使用者が所望するコンテンツを特定するコンテンツＩＤ、およびそのコンテンツを供給するコンテンツサーバ２２を特定するＵＲＬを受信する。

【００３０】

ポータブルデバイス２は、ライセンス管理プログラム８１、鍵管理プログラム８２、およびコンテンツ管理プログラム８３を実行する。

【００３１】

ライセンス管理プログラム８１は、コンテンツに対応する利用条件を基に、コンテンツの再生の回数などを管理する利用条件管理プログラム９１、パーソナルコンピュータ１を認証するPC認証プログラム９２、およびポータブルメディア３を認証するPM認証プログラム９３から構成される。

【００３２】

鍵管理プログラム８２は、パーソナルコンピュータ１から供給されたコンテンツ鍵を、ポータブルメディア３が予め記憶している保存用鍵で暗号化させ、ポータブルメディア３に記憶させて管理する。

【００３３】

コンテンツ管理プログラム８３は、パーソナルコンピュータ１から供給された

コンテンツを、ポータブルメディア３に記憶させて管理する。

【００３４】

ポータブルメディア３は、ライセンス管理プログラム１０１、鍵管理プログラム１０２、およびコンテンツ管理プログラム１０３を実行する。

【００３５】

ライセンス管理プログラム１０１は、ポータブルデバイス２を認証するPD認証プログラム１１１を有し、コンテンツに対応する利用条件のデータを記憶して、利用条件のデータに基づいて、コンテンツの読み出し等を制御する。鍵管理プログラム１０２は、ポータブルデバイス２から供給されたコンテンツ鍵を、予め記憶している保存用鍵で暗号化して記憶し、管理する。コンテンツ管理プログラム１０３は、ポータブルデバイス２から供給されたコンテンツを記憶して、管理する。

【００３６】

ショップサーバ２３は、鍵情報送信プログラム１２１、コンテンツ情報送信プログラム１２２、閲覧プログラム１２３、およびＩＰ通信プログラム１２４を実行する。

【００３７】

鍵情報送信プログラム１２１は、通信ネットワーク４を介して、パーソナルコンピュータ１に、パーソナルコンピュータ１の使用者が所望するコンテンツに対応するコンテンツ鍵を供給する鍵サーバ２１のＵＲＬを送信する。

【００３８】

コンテンツ情報送信プログラム１２２は、通信ネットワーク４を介して、パーソナルコンピュータ１に、パーソナルコンピュータ１の使用者が所望するコンテンツを供給するコンテンツサーバ２２のＵＲＬを送信する。

【００３９】

閲覧プログラム１２３は、コンテンツをパーソナルコンピュータ１の使用者に視聴させる視聴プログラム１３１、およびパーソナルコンピュータ１の使用者が所望のコンテンツを検索する検索プログラム１３２から構成されている。

【００４０】

ＩＰ通信プログラム１２４は、ＨＴＴＰ１３３およびＷａｐ１３４などの手続を包含し、通信ネットワーク４を介して、パーソナルコンピュータ１と通信するためのプログラムである。

【００４１】

鍵サーバ２１は、認証プログラム１５１、鍵配信プログラム１５２、鍵保存プログラム１５３、鍵生成プログラム１５４、およびＩＰ通信プログラム１５５を実行する。

【００４２】

認証プログラム１５１は、パーソナルコンピュータ１などを認証するプログラムである。鍵配信プログラム１５２は、認証されたパーソナルコンピュータ１に、鍵保存プログラム１５３が保存しているコンテンツ鍵を配信するプログラムである。鍵保存プログラム１５３は、鍵生成プログラム１５４により生成されたコンテンツ鍵を保存するプログラムである。鍵生成プログラム１５４は、コンテンツに対応させてコンテンツ鍵を生成するプログラムである。

【００４３】

ＩＰ通信プログラム１５５は、ＨＴＴＰ１７１およびＷａｐ１７２などの手続を包含し、通信ネットワーク４を介して、パーソナルコンピュータ１などと通信するためのプログラムである。

【００４４】

コンテンツサーバ２２は、コンテンツ保存プログラム１９１、コンテンツ配信プログラム１９２、およびＩＰ通信プログラム１９３を実行する。

【００４５】

コンテンツ保存プログラム１９１は、コンテンツ鍵で暗号化されているコンテンツをコンテンツＩＤと対応させて保存する。コンテンツ配信プログラム１９２は、パーソナルコンピュータ１から要求があったとき、コンテンツ保存プログラム１９１が保存している、コンテンツＩＤに対応するコンテンツをパーソナルコンピュータ１に配信する。

【００４６】

ＩＰ通信プログラム１９３は、ＨＴＴＰ２０１およびＷａｐ２０２などの手続

を包含し、通信ネットワーク４を介して、パーソナルコンピュータ１と通信するためのプログラムである。

【００４７】

次に、パーソナルコンピュータ１がコンテンツをダウンロードして、ポータブルデバイス２にチェックアウトする処理を図３および図４のフローチャートを参照して説明する。ステップＳ１０１において、パーソナルコンピュータ１のＰＨＳ／ＩＭＴ通信プログラム１５は、公衆回線網３１と接続を確立する。ステップＳ２０１において、公衆回線網３１の図示せぬ地上局などは、パーソナルコンピュータ１と接続を確立する。

【００４８】

ステップＳ１０２において、パーソナルコンピュータ１のＩＳＰ接続プログラム１４は、ＩＳＰ３２と接続を確立する。ステップＳ３０１において、ＩＳＰ３２は、パーソナルコンピュータ１と接続を確立する。

【００４９】

ステップＳ１０３において、パーソナルコンピュータ１のＩＰ通信プログラム１３は、ショップサーバ２３とＩＰ通信を確立する。ステップＳ４０１において、ショップサーバ２３のＩＰ通信プログラム１２４は、パーソナルコンピュータ１とＩＰ通信を確立する。

【００５０】

ステップＳ４０２において、ショップサーバ２３の閲覧プログラム１２３は、通信ネットワーク４を介して、パーソナルコンピュータ１に閲覧用（コンテンツの選択用）のデジタルデータを送信する。ステップＳ１０４において、パーソナルコンピュータ１の図示せぬブラウザプログラムは、デジタルデータに対応する画像またはテキストなどを表示し、使用者に閲覧させる。また、パーソナルコンピュータ１のブラウザプログラムは、コンテンツのストリーミング再生によりコンテンツを使用者に試聴させたり、または、キーワードによりコンテンツをショップサーバ２３の閲覧プログラム１２３に検索させ、その結果を表示する。ステップＳ４０２およびステップＳ１０４の処理は、パーソナルコンピュータ１の使用者の要求に対応して、繰り返される。

【００５１】

ステップＳ１０５において、パーソナルコンピュータ１のブラウザプログラムは、購入依頼をショップサーバ２３に送信する。ステップＳ４０３において、ショップサーバ２３の閲覧プログラム１２３は、パーソナルコンピュータ１から送信された購入依頼を受信する。

【００５２】

ステップＳ４０４において、ショップサーバ２３のコンテンツ情報送信プログラム１２２は、ステップＳ４０３の処理で受信した購入依頼に対応するコンテンツを配信するコンテンツサーバ２２のＵＲＬおよびコンテンツを特定するためのコンテンツＩＤなどを含む、コンテンツ情報を通信ネットワーク４を介してパーソナルコンピュータ１に送信する。ステップＳ１０６において、パーソナルコンピュータ１のコンテンツ情報受信プログラム５５は、ショップサーバ２３が送信した、コンテンツ情報を受信する。

【００５３】

ステップＳ４０５において、ショップサーバ２３の鍵情報送信プログラム１２１は、ステップＳ４０３の処理で受信した購入依頼に対応するコンテンツのコンテンツ鍵を配信する鍵サーバ２１のＵＲＬなどの、鍵情報を通信ネットワーク４を介してパーソナルコンピュータ１に送信する。ステップＳ１０７において、パーソナルコンピュータ１の鍵情報受信プログラム５４は、ショップサーバ２３が送信した鍵情報を受信する。

【００５４】

ステップＳ１０８において、パーソナルコンピュータ１のＩＰ通信プログラム１３は、ステップＳ１０６の処理で取得したコンテンツ情報に含まれるコンテンツサーバ２２のＵＲＬを基に、コンテンツサーバ２２とＩＰ通信を確立する。ステップＳ５０１において、コンテンツサーバ２２のＩＰ通信プログラム１９３は、パーソナルコンピュータ１とＩＰ通信を確立する。

【００５５】

ステップＳ１０９において、パーソナルコンピュータ１のコンテンツ管理プログラム５３は、ステップＳ１０６の処理で取得したコンテンツＩＤを、通信ネッ

トワーク４を介して、コンテンツサーバ２２に送信する。ステップＳ５０２において、コンテンツサーバ２２は、パーソナルコンピュータ１が送信したコンテンツＩＤを受信する。ステップＳ５０３において、コンテンツサーバ２２のコンテンツ配信プログラム１９２は、ステップＳ５０２で受信したコンテンツＩＤに対応するコンテンツ（暗号化されている）をコンテンツ保存プログラム１９１から読み出して、通信ネットワーク４を介して、パーソナルコンピュータ１に配信する。ステップＳ１１０において、パーソナルコンピュータ１のコンテンツ管理プログラム５３の受信プログラム６７は、コンテンツサーバ２２が送信したコンテンツを受信する。

【００５６】

ステップＳ１１１において、パーソナルコンピュータ１のＩＰ通信プログラム１３は、ステップＳ１０７の処理で取得した鍵情報に含まれる鍵サーバ２１のＵＲＬを基に、鍵サーバ２１とＩＰ通信を確立する。ステップＳ６０１において、鍵サーバ２１のＩＰ通信プログラム１５５は、パーソナルコンピュータ１とＩＰ通信を確立する。

【００５７】

ステップＳ１１２において、パーソナルコンピュータ１の鍵管理プログラム５２のサーバ認証プログラム６５は、鍵サーバ２１を認証する。ステップＳ６０２において、鍵サーバ２１の認証プログラム１５１は、パーソナルコンピュータ１を認証する。

【００５８】

鍵サーバ２１には、マスター鍵ＫMSが予め記憶されており、パーソナルコンピュータ１には、個別鍵ＫPPとパーソナルコンピュータ１のIDが予め記憶されている。パーソナルコンピュータ１には、更に、マスター鍵ＫMPが予め記憶されており、鍵サーバ２１にも鍵サーバ２１のIDと個別鍵ＫPSが記憶されている。

【００５９】

鍵サーバ２１は、パーソナルコンピュータ１から、パーソナルコンピュータ１のIDの供給を受け、そのIDと自分自身が有するマスター鍵ＫMSにハッシュ関数を適用して、パーソナルコンピュータ１の個別鍵ＫPPと同一の鍵を生成する。

【００６０】

パーソナルコンピュータ１は、鍵サーバ２１から、鍵サーバ２１のIDの供給を受け、そのIDと自分自身が有するマスター鍵ＫMPにハッシュ関数を適用して、鍵サーバ２１の個別鍵ＫPSと同一の鍵を生成する。このようにすることで、パーソナルコンピュータ１と鍵サーバ２１の両方に、共通の個別鍵が共有されることになる。これらの個別鍵を用いてさらに、一時鍵を生成する。

【００６１】

ステップＳ１１３において、パーソナルコンピュータ１の鍵管理プログラム５２は、コンテンツＩＤを鍵サーバ２１に送信する。ステップＳ６０３において、鍵サーバ２１は、パーソナルコンピュータ１が送信した、コンテンツＩＤを受信する。ステップＳ６０４において、鍵サーバ２１の鍵配信プログラム１５２は、鍵保存プログラム１５３がコンテンツＩＤと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク４を介して、そのコンテンツ鍵（一時鍵により暗号化されている）をパーソナルコンピュータ１に送信する。ステップＳ１１４において、パーソナルコンピュータ１の鍵管理プログラム５２の受信プログラム６６は、鍵サーバ２１が送信したコンテンツ鍵を受信する。鍵管理プログラム５２は、受信したコンテンツ鍵を一時鍵で復号する。

【００６２】

パーソナルコンピュータ１の使用者が、表示操作指示プログラム１１に対し、受信したコンテンツのチェックアウトを指示したとき、ステップＳ１１５以降の処理が実行される。

【００６３】

ステップＳ１１５において、パーソナルコンピュータ１のライセンス管理プログラム５１のPD認証プログラム６４は、ポータブルデバイス２を認証する。ステップＳ７０１において、ポータブルデバイス２のライセンス管理プログラム８１のPC認証プログラム９２は、パーソナルコンピュータ１を認証する。

【００６４】

ステップＳ１１５およびステップＳ７０１におけるパーソナルコンピュータ１とポータブルデバイス２との相互認証の処理は、チャレンジレスポンス方式の認

証の処理であり、ステップＳ１１２およびステップＳ６０２における鍵サーバ２１とパーソナルコンピュータ１との相互認証の処理に比較して、演算量が少ない。パーソナルコンピュータ１およびポータブルデバイス２は、それぞれ、同一の演算で、レスポンスから一時鍵を生成して、共有する。

【００６５】

ステップＳ１１６において、パーソナルコンピュータ１のコンテンツ管理プログラム５３は、暗号化されているコンテンツをポータブルデバイス２に配信する。ステップＳ７０２において、ポータブルデバイス２のコンテンツ管理プログラム８３は、パーソナルコンピュータ１が配信したコンテンツを受信して、ポータブルメディア３のコンテンツ管理プログラム１０３に供給する。ポータブルメディア３のコンテンツ管理プログラム１０３は、コンテンツを記憶する。

【００６６】

なお、ポータブルデバイス２とポータブルメディア３は、ポータブルデバイス２にポータブルメディア３が装着されたとき、相互認証する。

【００６７】

ステップＳ１１７において、パーソナルコンピュータ１の鍵管理プログラム５２は、ポータブルデバイス２に、ステップＳ１１６で配信したコンテンツに対応するコンテンツ鍵（ポータブルデバイス２とポータブルメディア３とで共有する一時鍵で暗号化されている）を配信する。ステップＳ７０３において、ポータブルデバイス２の鍵管理プログラム８２は、パーソナルコンピュータ１が配信したコンテンツ鍵を受信して、ポータブルメディア３の鍵管理プログラム１０２に供給する。ポータブルメディア３の鍵管理プログラム１０２は、コンテンツ鍵を一時鍵で復号して、コンテンツ鍵を記憶する。

【００６８】

【発明が解決しようとする課題】

しかしながら、パーソナルコンピュータ１に比較して、演算能力または記憶容量など処理能力が小さい、例えば、携帯型端末機が、コンテンツサーバ２２からコンテンツを直接ダウンロードし、鍵サーバ２１からコンテンツ鍵をダウンロードしようとすると、認証の処理の負荷が大きいので処理速度が遅く、実用に耐え

ない。

【００６９】

本発明はこのような状況に鑑みてなされたものであり、処理能力が小さくとも、不正なコンテンツの利用を防止しつつ、迅速に、コンテンツをダウンロードして利用できるようにすることを目的とする。

【００７０】

【課題を解決するための手段】

請求項１に記載の情報提供装置は、第１の情報処理装置を認証する第１の認証手段と、第２の情報処理装置を認証する第２の認証手段と、第１の情報処理装置からの、第２の情報処理装置を特定するデータおよび鍵の送信要求の受信を制御する受信制御手段と、第２の情報処理装置を特定するデータに基づき、第２の情報処理装置に鍵の送信要求を送信するとともに、第２の情報処理装置から鍵を受信するように通信を制御する通信制御手段と、第１の情報処理装置への鍵の送信を制御する送信制御手段とを含むことを特徴とする。

【００７１】

請求項２に記載の情報提供方法は、第１の情報処理装置を認証する第１の認証ステップと、第２の情報処理装置を認証する第２の認証ステップと、第１の情報処理装置からの、第２の情報処理装置を特定するデータおよび鍵の送信要求の受信を制御する受信制御ステップと、第２の情報処理装置を特定するデータに基づき、第２の情報処理装置に鍵の送信要求を送信するとともに、第２の情報処理装置から鍵を受信するように通信を制御する通信制御ステップと、第１の情報処理装置への鍵の送信を制御する送信制御ステップとを含むことを特徴とする。

【００７２】

請求項３に記載のプログラム格納媒体のプログラムは、第１の情報処理装置を認証する第１の認証ステップと、第２の情報処理装置を認証する第２の認証ステップと、第１の情報処理装置からの、第２の情報処理装置を特定するデータおよび鍵の送信要求の受信を制御する受信制御ステップと、第２の情報処理装置を特定するデータに基づき、第２の情報処理装置に鍵の送信要求を送信するとともに、第２の情報処理装置から鍵を受信するように通信を制御する通信制御ステップ

と、第１の情報処理装置への鍵の送信を制御する送信制御ステップとを含むことを特徴とする。

【００７３】

請求項４に記載の情報処理装置は、第１の情報提供装置を認証する認証手段と、第１の情報提供装置への、鍵を提供する第２の情報提供装置を特定するデータおよび鍵の送信要求の送信を制御する送信制御手段と、第２の情報提供装置から第１の情報提供装置が提供を受け、送信した鍵の受信を制御する受信制御手段とを含むことを特徴とする。

【００７４】

請求項５に記載の情報処理方法は、第１の情報提供装置を認証する認証ステップと、第１の情報提供装置への、鍵を提供する第２の情報提供装置を特定するデータおよび鍵の送信要求の送信を制御する送信制御ステップと、第２の情報提供装置から第１の情報提供装置が提供を受け、送信した鍵の受信を制御する受信制御ステップとを含むことを特徴とする。

【００７５】

請求項６に記載のプログラム格納媒体のプログラムは、第１の情報提供装置を認証する認証ステップと、第１の情報提供装置への、鍵を提供する第２の情報提供装置を特定するデータおよび鍵の送信要求の送信を制御する送信制御ステップと、第２の情報提供装置から第１の情報提供装置が提供を受け、送信した鍵の受信を制御する受信制御ステップとを含むことを特徴とする。

【００７６】

請求項１に記載の情報提供装置、請求項２に記載の情報提供方法、および請求項３に記載のプログラム格納媒体においては、第１の情報処理装置が認証され、第２の情報処理装置が認証され、第１の情報処理装置からの、第２の情報処理装置を特定するデータおよび鍵の送信要求の受信が制御され、第２の情報処理装置を特定するデータに基づき、第２の情報処理装置に鍵の送信要求を送信するとともに、第２の情報処理装置から鍵を受信するように通信が制御され、第１の情報処理装置への鍵の送信が制御される。

【００７７】

請求項４に記載の情報処理装置、請求項５に記載の情報処理方法、および請求項６に記載のプログラム格納媒体においては、第１の情報提供装置が認証され、第１の情報提供装置への、鍵を提供する第２の情報提供装置を特定するデータおよび鍵の送信要求の送信が制御され、第２の情報提供装置から第１の情報提供装置が提供を受け、送信した鍵の受信が制御される。

【００７８】

【発明の実施の形態】

図５は、本発明に係るデジタルデータ伝送システムの一実施の形態を示す図である。図１で説明した構成の場合と同一の部分には、図１の場合と同一の番号を付してあり、その説明は省略する。

【００７９】

電話機一体型端末機５０１は、ポータブルメディア３－１を装着可能に構成され、無線により、通信ネットワーク４に接続される。電話機一体型端末機５０１は、通信ネットワーク４を介して、コンテンツサーバ２２から受信したコンテンツ（所定の方式で圧縮され、暗号化されている）を、利用条件のデータ等と共にダウンロードして、コンテンツおよびその利用条件のデータを装着されているポータブルメディア３－１に記憶させる。

【００８０】

電話機一体型端末機５０１は、コンテンツに関連する利用条件のデータに基づいて、装着されているポータブルメディア３－１に記憶されているコンテンツを再生し、図示せぬヘッドフォンまたはスピーカなどに出力する。使用者は、電話機一体型端末機５０１を持ち歩きながら、所望の場所で所望のコンテンツをダウンロードして、そのコンテンツをポータブルメディア３に記憶させることができる。使用者は、電話機一体型端末機５０１に、ポータブルメディア３に記憶されているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【００８１】

電話機一体型端末機５０１の表示操作指示プログラム５１１は、コンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、

ダウンロードの指示などを入力して、クライアント用ＬＣＭ５１２にその指示に対応した処理を実行させる。電話機一体型端末機５０１のクライアント用ＬＣＭ５１２は、認証サーバ５０３のサーバ用ＬＣＭ５１４と協同して、利用条件データおよびコンテンツ等をダウンロードする一連の処理（後述する）を実行する。

【００８２】

電話機一体型端末機５０１のクライアント用ＬＣＭ５１２は、コンテンツの不正な２次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

【００８３】

クライアント用ＬＣＭ５１２は、電話機一体型端末機５０１に装着されているポータブルメディア３－１が正当であるかの認証を行い、安全な方法でサーバ５が指定した利用条件のデータをコンテンツ（暗号化されている）に付加して、ポータブルメディア３－１にコンテンツを記録させる。コンテンツの移動の処理などに伴い、クライアント用ＬＣＭ５１２は、必要な鍵を生成して、鍵を管理し、または接続されているポータブルメディア３－１との通信を制御する。

【００８４】

パーソナルコンピュータ５０２は、通信ネットワーク４に接続されている。パーソナルコンピュータ５０２は、コンテンツサーバ２２から受信した、またはCDから読み取ったコンテンツを、所定の圧縮の方式に変換するとともにDESなどの暗号化方式で暗号化して記録する。パーソナルコンピュータ５０２は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

【００８５】

パーソナルコンピュータ５０２の表示操作指示プログラム１１は、コンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、ダウンロード、またはチェックアウトの指示などを入力して、ＬＣＭ５１３にその指示に対応したダウンロード、またはチェックアウトなどの処理を実行させ

る。

【００８６】

パーソナルコンピュータ５０２のＬＣＭ５１３は、コンテンツの不正な２次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

【００８７】

ＬＣＭ５１３は、パーソナルコンピュータ５０２に接続されたポータブルデバイス２が正当であるかの認証を行い、安全な方法でコンテンツの移動の処理などを実行する。コンテンツの移動の処理などに伴い、ＬＣＭ５１３は、必要な鍵を生成して、鍵を管理し、コンテンツを暗号化し、または接続されている機器との通信を制御する。

【００８８】

また、ＬＣＭ５１３は、ポータブルデバイス２の正当性をチェックする。ポータブルデバイス２は、ポータブルメディア３－２が装着されたとき、ポータブルメディア３－２の正当性をチェックする。ポータブルデバイス２およびポータブルメディア３－２が正当である場合、ＬＣＭ５１３は、サーバ５が指定した利用条件のデータをコンテンツ（暗号化されている）に付加して、ポータブルメディア３－２にコンテンツをチェックアウトする。ポータブルデバイス２は、パーソナルコンピュータ５０２からチェックアウトされたコンテンツを、コンテンツに関連するデータと共に、装着されているポータブルメディア３－２に記憶させる。

【００８９】

認証サーバ５０３を利用できるとき、パーソナルコンピュータ５０２のＰＣ用ＬＣＭ５２１（ＬＣＭ５１３の一部または全部の機能から構成される）は、認証サーバ５０３のサーバ用ＬＣＭ５１４と協同して、利用条件データおよびコンテンツ等をダウンロードする一連の処理を実行する。

【００９０】

認証サーバ５０３を利用できないとき、パーソナルコンピュータ５０２のＬＣＭ５１３は、ＬＣＭ１２と同様の鍵サーバ２１との認証の処理等を実行して、利用条件データおよびコンテンツ等をダウンロードする。

【００９１】

認証サーバ５０３は、サーバ用ＬＣＭ５１４を実行して、相互認証した電話機一体型端末機５０１または相互認証したパーソナルコンピュータ５０２の要求に対応して、鍵サーバ２１との認証の処理を実行する。認証サーバ５０３は、鍵サーバ２１との相互認証の処理の後、鍵サーバ２１からコンテンツ鍵を受信して、受信したコンテンツ鍵を電話機一体型端末機５０１またはパーソナルコンピュータ５０２に供給する。

【００９２】

電話機一体型端末機５０１またはパーソナルコンピュータ５０２は、鍵サーバ２１との認証の処理の実行を必要とせず、鍵サーバ２１との認証の処理に比較してより処理の負荷の小さい認証サーバ５０３との認証の処理を実行するだけで、コンテンツ鍵を取得することができる。

【００９３】

図６は、電話機一体型端末機５０１の構成を説明する図である。CPU (Central Processing Unit) ６０１は、ROM (Read-only Memory) ６０２またはRAM (Random-Access Memory) ６０３に格納されている各種プログラムを実際に実行する。ROM６０２は、EEPROM (Electrically Erasable Programmable Read-Only Memory) またはフラッシュメモリなどで構成され、一般的には、CPU６０１が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM６０３は、SRAM (Static RAM) などで構成され、CPU６０１の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。

【００９４】

入力部６０５は、入力キーまたはマイクロフォンなどで構成され、CPU６０１に各種の指令を入力するとき、または音声などを入力するとき、使用者により操作される。表示部６０６は、液晶表示装置などから成り、各種情報をテキストやイメージで表示する。

【００９５】

音声再生部６０７は、通信部６０８から供給された通話相手の音声のデータ、またはインターフェース６０９から供給されたポータブルメディア３－１に記憶されているコンテンツを再生して、音声を出力する。

【００９６】

通信部６０８は、公衆回線網３１と接続し、CPU６０１から供給されたデータ（例えば、コンテンツの送信要求など）または入力部６０５から供給された使用者の音声のデータを、所定の方式のパケットに格納して、公衆回線網３１を介して、送信する。また、通信部６０８は、公衆回線網３１を介して、受信したパケットに格納されているデータ（例えば、コンテンツなど）または通話相手の音声のデータをCPU６０１、RAM６０３、音声再生部６０７、またはインターフェース６０９に出力する。

【００９７】

インターフェース６０９は、CPU６０１、RAM６０３、または通信部６０８から供給されたデータを装着されているポータブルメディア３－１に記憶させるとともに、装着されているポータブルメディア３－１からコンテンツなどのデータを読み出して、CPU６０１、RAM６０３、または音声再生部６０７に供給する。

【００９８】

インターフェース６１０は、外付けのドライブ６３１が接続される。ドライブ６３１は、装着されている磁気ディスク６４１、光ディスク６４２（CD-ROMを含む）、光磁気ディスク６４３、または半導体メモリ６４４に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース６１０、およびバス６０４を介して接続されているROM６０２またはRAM６０３に供給する。

【００９９】

CPU６０１乃至インターフェース６１０は、バス６０４により相互に接続されている。

【０１００】

図７は、認証サーバ５０３の構成を説明する図である。CPU６５１は、各種ア

プリケーションプログラム（詳細については後述する）や、OS（Operating System)を実際に実行する。ROM６５２は、一般的には、CPU６５１が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM６５３は、CPU６５１の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはCPUバスなどから構成されるホストバス６５４により相互に接続されている。

【０１０１】

ホストバス６５４は、ブリッジ６５５を介して、PCI(Peripheral Component Interconnect/Interface)バスなどの外部バス６５６に接続されている。

【０１０２】

キーボード６５８は、CPU６５１に各種の指令を入力するとき、使用者により操作される。ポインティングデバイス６５９は、ディスプレイ６６０の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ６６０は、液晶表示装置またはCRT（Cathode Ray Tube）などから成り、各種情報をテキストやイメージで表示する。HDD（Hard Disk Drive）６６１は、ハードディスクを駆動し、それらにCPU６５１によって実行するプログラムや情報を記録または再生させる。

【０１０３】

ドライブ６６２は、装着されている磁気ディスク６８１、光ディスク６８２、光磁気ディスク６８３、または半導体メモリ６８４に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース６５７、外部バス６５６、ブリッジ６５５、およびホストバス６５４を介して接続されているRAM６５３に供給する。

【０１０４】

これらのキーボード６５８乃至ドライブ６６２は、インターフェース６５７に接続されており、インターフェース６５７は、外部バス６５６、ブリッジ６５５、およびホストバス６５４を介してCPU６５１に接続されている。

【０１０５】

通信部６６３は、通信ネットワーク４が接続され、CPU６５１、またはHDD６６

１から供給されたデータ（例えば、コンテンツ鍵など）を、所定の方式のパケットに格納して、通信ネットワーク４を介して、送信するとともに、通信ネットワーク４を介して、受信したパケットに格納されているデータ（例えば、コンテンツＩＤなど）をCPU６５１、RAM６５３、またはHDD６６１に出力する。

【０１０６】

通信部６６３は、外部バス６５６、ブリッジ６５５、およびホストバス６５４を介してCPU６５１に接続されている。

【０１０７】

次に、図８を参照して、本願のデジタルデータ伝送システムの機能の構成について説明する。図２で説明した構成の場合と同一の部分には、図２の場合と同一の番号を付してあり、その説明は省略する。

【０１０８】

電話機一体型端末機５０１は、表示操作指示プログラム５１１、クライアント用ＬＣＭ５１２、ＩＰ通信プログラム７０１、ＩＳＰ接続プログラム７０２、およびＰＨＳ／ＩＭＴ通信プログラム７０３を実行する。

【０１０９】

ＰＨＳ／ＩＭＴ通信プログラム７０３は、公衆回線網３１を介して通信を行うためのプログラムである。ＩＳＰ接続プログラム７０２は、ＩＳＰ３２と接続するためのプログラムである。ＩＰ通信プログラム７０１は、ＨＴＴＰ７３１およびＷａｐ７３２などの手続を包含し、通信ネットワーク４を介して、鍵サーバ２１、コンテンツサーバ２２、ショップサーバ２３、または認証サーバ５０３などと通信するためのプログラムである。

【０１１０】

クライアント用ＬＣＭ５１２は、ライセンス管理プログラム７１１、鍵管理プログラム７１２、コンテンツ管理プログラム７１３、鍵情報受信プログラム７１４、およびコンテンツ情報受信プログラム７１５などから構成されている。

【０１１１】

ライセンス管理プログラム７１１は、コンテンツの利用条件に基づいたコンテンツの利用を管理するためのプログラムであり、利用条件管理プログラム７２１

、サーバ認証プログラム７２２、およびPM認証プログラム７２３から構成されている。

【０１１２】

利用条件管理プログラム７２１は、コンテンツの利用条件に基づいて、ポータブルメディア３－１が記憶しているコンテンツの再生などを許可するか、または禁止するかなどの管理を実行するとともに、ポータブルメディア３－１が記憶しているコンテンツの再生などに対応して、ポータブルメディア３－１に、ポータブルメディア３－１が記憶している利用条件のデータを更新させる。サーバ認証プログラム７２２は、通信ネットワーク４を介して、認証サーバ５０３を認証する。PM認証プログラム７２３は、ポータブルメディア３－１が電話機一体型端末機５０１に装着されたとき、ポータブルメディア３－１を認証する。

【０１１３】

鍵管理プログラム７１２は、認証サーバ５０３からコンテンツ鍵を受信して、コンテンツに対応させて、コンテンツ鍵をポータブルメディア３－１に記憶させて、管理する。鍵管理プログラム７１２は、認証サーバ５０３からコンテンツ鍵を受信する受信プログラム７２４などを含む。

【０１１４】

コンテンツ管理プログラム７１３は、コンテンツサーバ２２からコンテンツの利用条件とともにコンテンツ（暗号化されている）を受信して、コンテンツの利用条件とともにコンテンツをポータブルメディア３－１に記憶させる。コンテンツ管理プログラム７１３の受信プログラム７２５は、コンテンツサーバ２２からコンテンツの利用条件およびコンテンツを受信する。

【０１１５】

鍵情報受信プログラム７１４は、ショップサーバ２３から、コンテンツに対応するコンテンツ鍵を供給する鍵サーバ２１を特定するＵＲＬを受信する。コンテンツ情報受信プログラム７１５は、ショップサーバ２３から、所望のコンテンツを特定するコンテンツＩＤ、および所望のコンテンツを供給するコンテンツサーバ２２を特定するＵＲＬを受信する。

【０１１６】

認証サーバ５０３は、サーバ用ＬＣＭ５１４、およびＩＰ通信プログラム７４１を実行する。

【０１１７】

サーバ用ＬＣＭ５１４は、ライセンス管理プログラム７５１、および鍵管理プログラム７５２などを含む。

【０１１８】

ライセンス管理プログラム７５１は、更に、鍵サーバ２１を認証するサーバ認証プログラム７６１、および電話機一体型端末機５０１を認証するＰＤ認証プログラム７６２などを含む。

【０１１９】

鍵管理プログラム７５２は、更に、通信ネットワーク４を介して、鍵サーバ２１からコンテンツ鍵を受信する鍵受信プログラム７６３、および通信ネットワーク４を介して、受信したコンテンツ鍵を電話機一体型端末機５０１に配信する鍵配信プログラム７６４などを含む。

【０１２０】

ＩＰ通信プログラム７４１は、ＨＴＴＰ７６５およびＷａｐ７６６などの手続を包含し、通信ネットワーク４を介して、鍵サーバ２１または電話機一体型端末機５０１と通信するためのプログラムである。

【０１２１】

次に、電話機一体型端末機５０１がコンテンツをダウンロードする処理を図９および図１０のフローチャートを参照して説明する。ステップＳ１００１において、電話機一体型端末機５０１のＰＨＳ／ＩＭＴ通信プログラム７０３は、公衆回線網３１と接続を確立する。ステップＳ１１０１において、公衆回線網３１の図示せぬ地上局などは、電話機一体型端末機５０１と接続を確立する。

【０１２２】

ステップＳ１００２において、電話機一体型端末機５０１のＩＳＰ接続プログラム７０２は、電話機一体型端末機５０１と公衆回線網３１との接続を介して、ＩＳＰ３２と接続を確立する。ステップＳ１２０１において、ＩＳＰ３２は、電話機一体型端末機５０１と公衆回線網３１との接続を介して、電話機一体型端末

機５０１と接続を確立する。

【０１２３】

以降の電話機一体型端末機５０１と、鍵サーバ２１、コンテンツサーバ２２、ショップサーバ２３、または認証サーバ５０３との処理は、電話機一体型端末機５０１とＩＳＰ３２との接続を介して実行される。

【０１２４】

ステップＳ１００３において、電話機一体型端末機５０１のＩＰ通信プログラム７０１は、ショップサーバ２３とＩＰ通信を確立する。ステップＳ１３０１において、ショップサーバ２３のＩＰ通信プログラム１２４は、電話機一体型端末機５０１とＩＰ通信を確立する。

【０１２５】

ステップＳ１３０２において、ショップサーバ２３の閲覧プログラム１２３は、通信ネットワーク４を介して、電話機一体型端末機５０１に閲覧用（コンテンツの選択用）のデジタルデータを送信する。ステップＳ１００４において、電話機一体型端末機５０１の図示せぬブラウザプログラムは、受信したデジタルデータに対応するテキストまたは画像を表示部６０６に表示させ、使用者に閲覧させる。また、電話機一体型端末機５０１のブラウザプログラムは、コンテンツのストリーミング再生により、コンテンツを音声再生部６０７に再生させて、使用者に試聴させたり、または、キーワードにより所望のコンテンツをショップサーバ２３の閲覧プログラム１２３に検索させ、その結果を表示部６０６に表示させる。

【０１２６】

ステップＳ１３０２およびステップＳ１００４の処理は、電話機一体型端末機５０１の使用者の要求に対応して、例えば、使用者が購入するコンテンツを決定するまで繰り返される。

【０１２７】

ステップＳ１００５において、電話機一体型端末機５０１のブラウザプログラムは、通信ネットワーク４を介して、購入依頼をショップサーバ２３に送信する。ステップＳ１３０３において、ショップサーバ２３の閲覧プログラム１２３は

、電話機一体型端末機５０１から送信された購入依頼を受信する。

【０１２８】

ステップＳ１３０４において、ショップサーバ２３のコンテンツ情報送信プログラム１２２は、ステップＳ１３０３の処理で受信した購入依頼に対応して、コンテンツを配信するコンテンツサーバ２２のＵＲＬ、およびコンテンツを特定するためのコンテンツＩＤなどを含む、コンテンツ情報を、通信ネットワーク４を介して、電話機一体型端末機５０１に送信する。ステップＳ１００６において、電話機一体型端末機５０１のコンテンツ情報受信プログラム７１５は、ショップサーバ２３が送信した、コンテンツ情報を受信する。

【０１２９】

ステップＳ１３０５において、ショップサーバ２３の鍵情報送信プログラム１２１は、ステップＳ１３０３の処理で受信した購入依頼に対応するコンテンツのコンテンツ鍵を配信する鍵サーバ２１のＵＲＬなどの、鍵情報を通信ネットワーク４を介して、電話機一体型端末機５０１に送信する。ステップＳ１００７において、電話機一体型端末機５０１の鍵情報受信プログラム７１４は、ショップサーバ２３が送信した、鍵情報を受信する。

【０１３０】

ステップＳ１００８において、電話機一体型端末機５０１のＩＰ通信プログラム７０１は、ステップＳ１００６の処理で取得したコンテンツ情報に含まれるコンテンツサーバ２２のＵＲＬを基に、コンテンツサーバ２２とＩＰ通信を確立する。ステップＳ１４０１において、コンテンツサーバ２２のＩＰ通信プログラム１９３は、電話機一体型端末機５０１とＩＰ通信を確立する。

【０１３１】

ステップＳ１００９において、電話機一体型端末機５０１のコンテンツ管理プログラム７１３は、ステップＳ１００６の処理で取得したコンテンツＩＤを、通信ネットワーク４を介して、コンテンツサーバ２２に送信する。ステップＳ１４０２において、コンテンツサーバ２２は、電話機一体型端末機５０１が送信したコンテンツＩＤを受信する。ステップＳ１４０３において、コンテンツサーバ２２のコンテンツ配信プログラム１９２は、ステップＳ１４０２で受信したコンテ

ンツＩＤに対応するコンテンツ（暗号化されている）を、コンテンツ保存プログラム１９１から読み出して、通信ネットワーク４を介して、電話機一体型端末機５０１に配信する。

【０１３２】

ステップＳ１０１０において、電話機一体型端末機５０１のコンテンツ管理プログラム７１３の受信プログラム７２５は、コンテンツサーバ２２が送信したコンテンツを受信する。コンテンツ管理プログラム７１３は、受信したコンテンツを、インターフェース６０９を介して、ポータブルメディア３－１に供給して、コンテンツ管理プログラム１０３に、コンテンツを記憶させる。

【０１３３】

ステップＳ１０１１において、電話機一体型端末機５０１のＩＰ通信プログラム７０１は、ステップＳ１００７の処理で取得した鍵情報に含まれる鍵サーバ２１のＵＲＬを基に、認証サーバ５０３とＩＰ通信を確立する。ステップＳ１５０１において、認証サーバ５０３のＩＰ通信プログラム７４１は、電話機一体型端末機５０１とＩＰ通信を確立する。

【０１３４】

ステップＳ１０１２において、電話機一体型端末機５０１のライセンス管理プログラム７１１のサーバ認証プログラム７２２は、認証サーバ５０３を認証する。ステップＳ１５０２において、認証サーバ５０３のライセンス管理プログラム７５１のPD認証プログラム７６２は、電話機一体型端末機５０１を認証する。

【０１３５】

ステップＳ１０１２およびステップＳ１５０２における電話機一体型端末機５０１と認証サーバ５０３との相互認証の処理は、チャレンジレスポンス方式の認証の処理であり、ステップＳ１１２およびステップＳ６０２における鍵サーバ２１とパーソナルコンピュータ１との相互認証の処理に比較して、演算量が少なく、少ない演算能力、または記憶容量でも、迅速に実行することができる。電話機一体型端末機５０１および認証サーバ５０３は、それぞれ、同一の演算で、レスポンスから一時鍵を生成して、共有する。

【０１３６】

ステップＳ１０１２またはステップＳ１５０２における認証の処理に失敗したとき（認証の相手が正当でないと判定されたとき）、電話機一体型端末機５０１がコンテンツをダウンロードする処理は、コンテンツ鍵が電話機一体型端末機５０１にダウンロードされずに終了するので、電話機一体型端末機５０１は、コンテンツを利用することができない。

【０１３７】

ステップＳ１０１３において、電話機一体型端末機５０１の鍵管理プログラム７１２は、コンテンツＩＤを認証サーバ５０３に送信する。ステップＳ１５０３において、認証サーバ５０３は、電話機一体型端末機５０１が送信したコンテンツＩＤを受信する。ステップＳ１０１４において、電話機一体型端末機５０１の鍵管理プログラム７１２は、ステップＳ１００７の処理で受信した鍵情報を認証サーバ５０３に送信する。ステップＳ１５０４において、認証サーバ５０３は、電話機一体型端末機５０１が送信した、鍵情報を受信する。

【０１３８】

ステップＳ１５０５において、認証サーバ５０３のＩＰ通信プログラム７４１は、鍵サーバ２１とＩＰ通信を確立する。ステップＳ１６０１において、鍵サーバ２１のＩＰ通信プログラム１５５は、認証サーバ５０３とＩＰ通信を確立する。

【０１３９】

ステップＳ１０１６において、認証サーバ５０３のライセンス管理プログラム７５１のサーバ認証プログラム７６１は、鍵サーバ２１を認証する。ステップＳ１６０２において、鍵サーバ２１の認証プログラム１５１は、認証サーバ５０３を認証する。

【０１４０】

例えば、鍵サーバ２１には、マスター鍵ＫMSSが予め記憶されており、認証サーバ５０３には、個別鍵ＫPCCと認証サーバ５０３のIDが予め記憶されている。認証サーバ５０３には、更に、マスター鍵ＫMCCが予め記憶されており、鍵サーバ２１にも鍵サーバ２１のIDと個別鍵ＫPSSが記憶されている。

【０１４１】

鍵サーバ２１は、認証サーバ５０３から、認証サーバ５０３のIDの供給を受け、そのIDと自分自身が有するマスター鍵ＫMSSにハッシュ関数を適用して、認証サーバ５０３の個別鍵ＫPCCと同一の鍵を生成する。

【０１４２】

認証サーバ５０３は、鍵サーバ２１から、鍵サーバ２１のIDの供給を受け、そのIDと自分自身が有するマスター鍵ＫMCCにハッシュ関数を適用して、鍵サーバ２１の個別鍵ＫPSSと同一の鍵を生成する。このようにすることで、認証サーバ５０３と鍵サーバ２１の両方に、共通の個別鍵が共有されることになる。これらの個別鍵を用いてさらに、一時的な一時鍵を生成する。

【０１４３】

ステップＳ１５０６またはステップＳ１６０２における認証の処理に失敗したとき（認証の相手が正当でないと判定されたとき）、電話機一体型端末機５０１がコンテンツをダウンロードする処理は、コンテンツ鍵が電話機一体型端末機５０１にダウンロードされずに終了するので、電話機一体型端末機５０１は、コンテンツを利用することができない。

【０１４４】

ステップＳ１５０７において、認証サーバ５０３の鍵管理プログラム７５２は、ステップＳ１５０３の処理で取得したコンテンツＩＤを鍵サーバ２１に送信する。ステップＳ１６０３において、鍵サーバ２１は、認証サーバ５０３が送信したコンテンツＩＤを受信する。ステップＳ１６０４において、鍵サーバ２１の鍵配信プログラム１５２は、鍵保存プログラム１５３がコンテンツＩＤと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク４を介して、そのコンテンツ鍵（鍵サーバ２１と認証サーバ５０３とで共有する一時鍵で暗号化されている）を認証サーバ５０３に送信する。ステップＳ１５０８において、認証サーバ５０３の鍵管理プログラム７５２の鍵受信プログラム７６３は、鍵サーバ２１が送信したコンテンツ鍵を受信する。

【０１４５】

ステップＳ１５０９において、認証サーバ５０３の鍵管理プログラム７５２の鍵配信プログラム７６４は、ステップＳ１５０８の処理で受信したコンテンツ鍵

を、鍵サーバ２１と認証サーバ５０３とで共有する一時鍵で復号し、電話機一体型端末機５０１と認証サーバ５０３で共有する一時鍵で暗号化して、通信ネットワーク４を介して、暗号化されているコンテンツ鍵を電話機一体型端末機５０１に送信する。ステップＳ１０１５において、電話機一体型端末機５０１の鍵管理プログラム７１２の受信プログラム７２４は、認証サーバ５０３が送信したコンテンツ鍵を受信する。鍵管理プログラム７１２は、コンテンツ鍵を電話機一体型端末機５０１と認証サーバ５０３で共有する一時鍵で復号して、ポータブルメディア３の鍵管理プログラム１０２に供給し、鍵管理プログラム１０２に、コンテンツ鍵を記憶させる。

【０１４６】

ステップＳ１０１２およびステップＳ１５０２における電話機一体型端末機５０１と認証サーバ５０３との相互認証の処理は、電話機一体型端末機５０１と鍵サーバ２１が相互認証する場合の処理に比較して、演算量が少なく、高い演算能力、または大きな記憶容量などを必要としない。従って、相互認証を実行することにより不正なコンテンツの利用を防止しつつ、電話機一体型端末機５０１は、処理能力が小さくとも、迅速に、コンテンツをダウンロードして利用できる。

【０１４７】

さらに、電話機一体型端末機５０１は、コンテンツのダウンロードと同時に、コンテンツをポータブルメディア３に記憶させることができるので、使用者は、電話機一体型端末機５０１に対してチェックアウトなどの操作を指示する必要がなく、迅速に、コンテンツを利用することができる。

【０１４８】

また、サーバ用ＬＣＭ５１４の更新（例えば、バージョンアップ）は、認証サーバ５０３の管理者が一元的に迅速に行うことができる。さらに、クライアント用ＬＣＭ５１２は、従来のＬＣＭ１２に比較して、小さなプログラムとなるので（例えば、サーバ認証プログラム７２２は、従来のサーバ認証プログラム６５に比較して小さくインプリメントできる。）、電話機一体型端末機５０１は、クライアント用ＬＣＭ５１２を更新する処理を迅速に行うことができる。

【０１４９】

なお、認証サーバ５０３を利用することができるとき、パーソナルコンピュータ５０２のＰＣ用ＬＣＭ５２１は、上述した電話機一体型端末機５０１のクライアント用ＬＣＭ５１２と同様の処理を実行する。認証サーバ５０３を利用することができないとき、パーソナルコンピュータ５０２のＬＣＭ５１３は、従来のＬＣＭ１２と同様の処理を実行する。

【０１５０】

また、コンテンツは、楽音のデータであると説明したが、楽音のデータに限らず、静止画像のデータ、動画像のデータ、テキストのデータ、またはプログラムなどでもよい。

【０１５１】

なお、電話機一体型端末機５０１またはパーソナルコンピュータ５０２が、コンテンツをダウンロードすると説明したが、電話機一体型端末機５０１またはパーソナルコンピュータ５０２に限らず、携帯電話機、ＰＤＡ（Personal Digital Assistant）、通信機能付き撮像機能付きデジタルビデオカセットレコーダ、通信機能付き電子手帳装置、または携帯型パーソナルコンピュータなどがコンテンツをダウンロードするようにしてもよい。

【０１５２】

また、電話機一体型端末機５０１は、ＰＨＳまたはＩＭＴにより通信すると説明したが、ＰＨＳまたはＩＭＴに限らず、W-CDMA（Code Division Multiple Access）、衛星通信、衛星放送、PSTN（Public Switched telephone network）、xDSL（x Digital Subscriber Line）、ISDN（Integrated Services Digital Network）、またはプライベートネットワークなどで通信するようにしてもよい。

【０１５３】

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

【０１５４】

コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図６または図７に示すように、磁気ディスク６４１若しくは磁気ディスク６８１（いずれもフロッピディスクを含む）、光ディスク６４２若しくは光ディスク６８２（いずれも、CD-ROM(Compact Disc-Read Only Memory)、ＤＶＤ(Digital Versatile Disc)を含む）、光磁気ディスク６４３若しくは光磁気ディスク６８３（いずれもＭＤ(Mini-Disc)を含む）、若しくは半導体メモリ６４４若しくは半導体メモリ６８４などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納されるROM６０２若しくはROM６５２や、HDD６６１などにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じて通信部６０８または通信部６６３を介して、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【０１５５】

なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０１５６】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０１５７】

【発明の効果】

請求項１に記載の情報提供装置、請求項２に記載の情報提供方法、および請求項３に記載のプログラム格納媒体によれば、第１の情報処理装置が認証され、第２の情報処理装置が認証され、第１の情報処理装置からの、第２の情報処理装置を特定するデータおよび鍵の送信要求の受信が制御され、第２の情報処理装置を特定するデータに基づき、第２の情報処理装置に鍵の送信要求を送信するとともに、第２の情報処理装置から鍵を受信するように通信が制御され、第１の情報処

理装置への鍵の送信が制御されるようにしたので、第１の情報処理装置は、処理能力が小さくとも、不正なコンテンツの利用を防止しつつ、迅速に、コンテンツをダウンロードして利用できるようになる。

【０１５８】

請求項４に記載の情報処理装置、請求項５に記載の情報処理方法、および請求項６に記載のプログラム格納媒体においては、第１の情報提供装置が認証され、第１の情報提供装置への、鍵を提供する第２の情報提供装置を特定するデータおよび鍵の送信要求の送信が制御され、第２の情報提供装置から第１の情報提供装置が提供を受け、送信した鍵の受信が制御されるようにしたので、処理能力が小さくとも、不正なコンテンツの利用を防止しつつ、迅速に、コンテンツをダウンロードして利用できるようになる。

【図面の簡単な説明】

【図１】

従来のデジタルデータ伝送システムの構成を示す図である。

【図２】

従来のデジタルデータ伝送システムの機能の構成を示す図である。

【図３】

パーソナルコンピュータ１がコンテンツをダウンロードして、ポータブルデバイス２にチェックアウトする処理を説明するフローチャートである。

【図４】

パーソナルコンピュータ１がコンテンツをダウンロードして、ポータブルデバイス２にチェックアウトする処理を説明するフローチャートである。

【図５】

本発明に係るデジタルデータ伝送システムの一実施の形態を示す図である。

【図６】

電話機一体型端末機５０１の構成を説明する図である。

【図７】

認証サーバ５０３の構成を説明する図である。

【図８】

本願のデジタルデータ伝送システムの機能の構成を説明する図である。

【図９】

電話機一体型端末機５０１がコンテンツをダウンロードする処理を説明するフローチャートである。

【図１０】

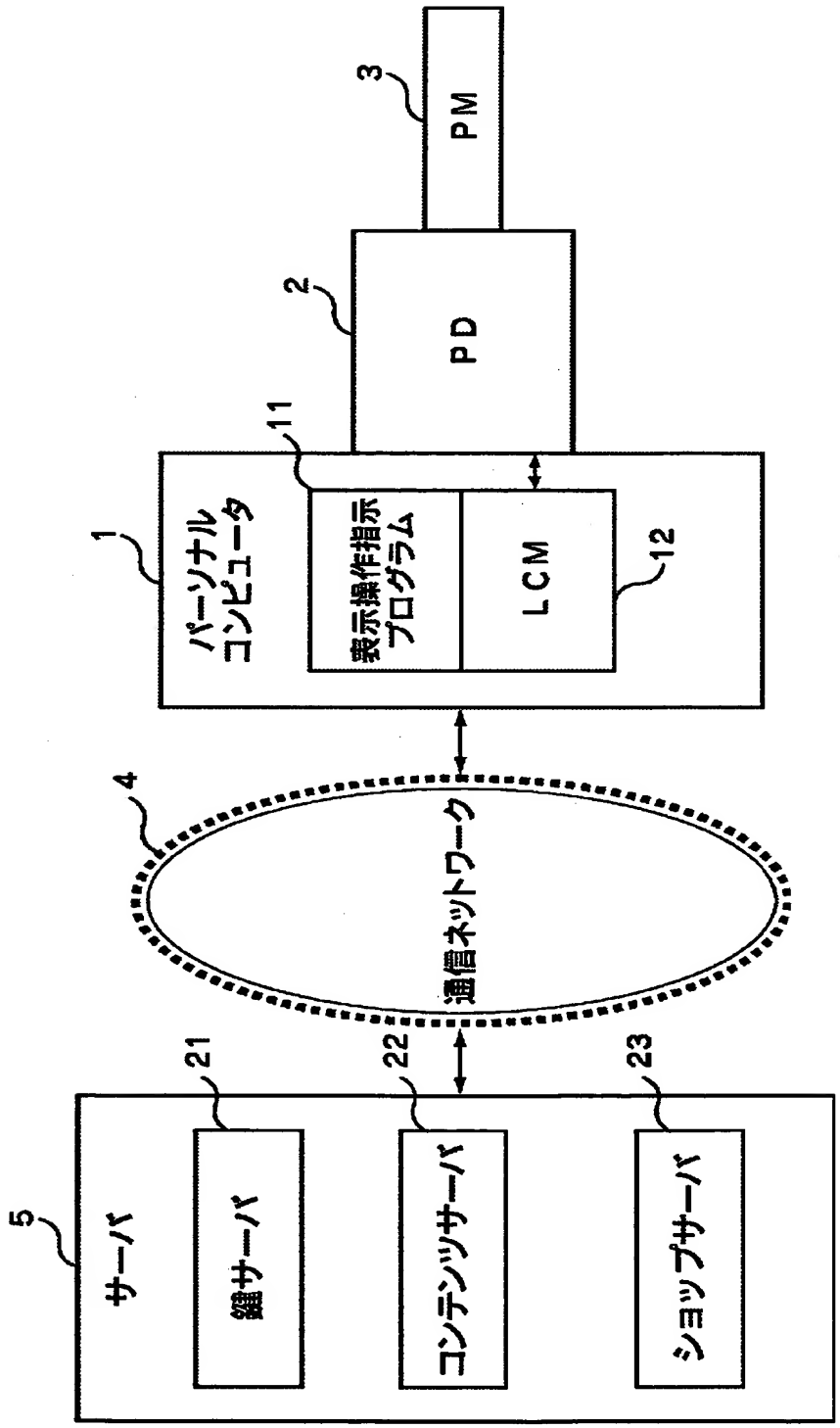
電話機一体型端末機５０１がコンテンツをダウンロードする処理を説明するフローチャートである。

【符号の説明】

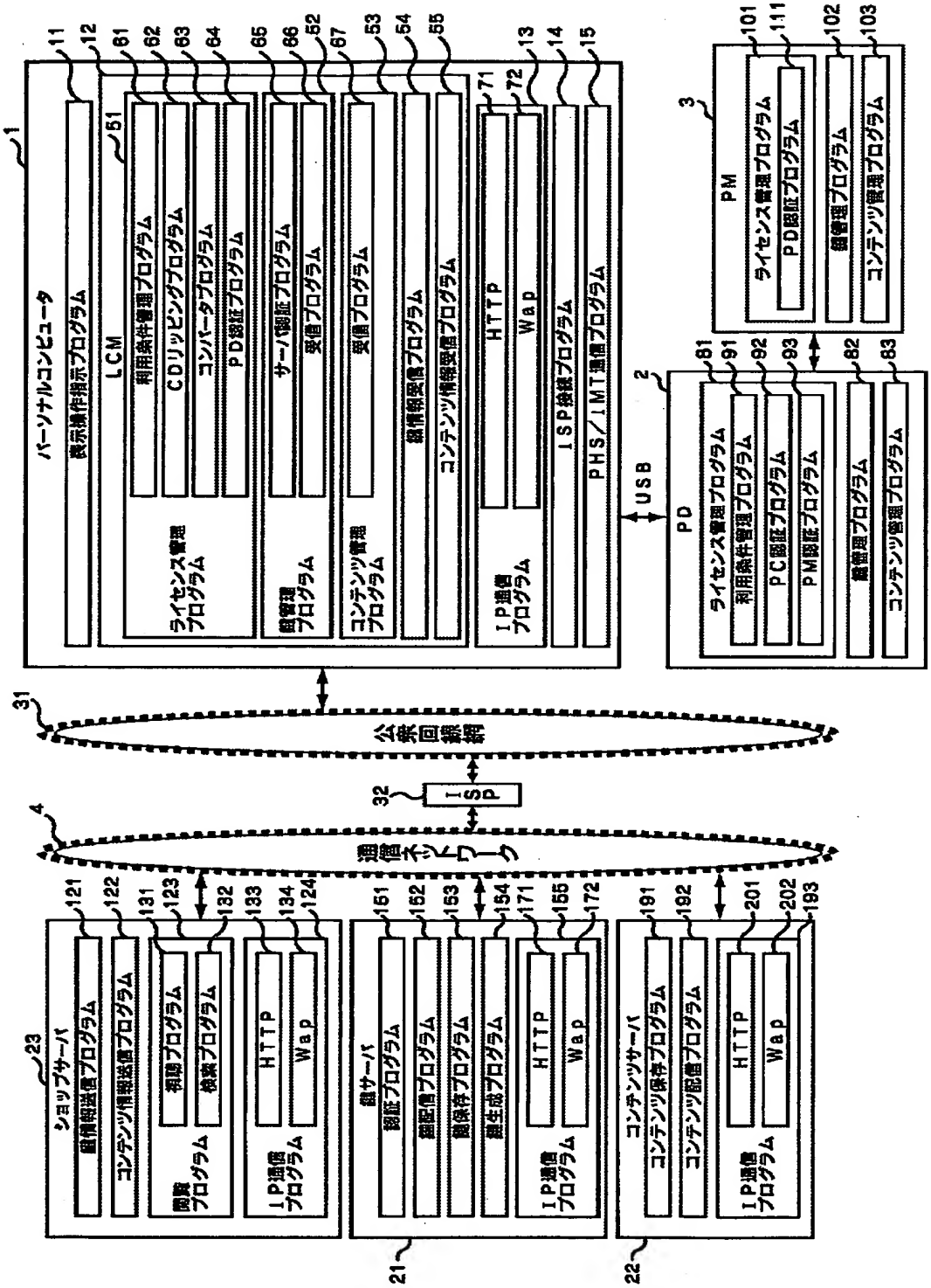
５０１　電話機一体型端末機，　５０３　認証サーバ，　５１１　表示操作指示プログラム，　５１２　クライアント用ＬＣＭ，　５１４　サーバ用ＬＣＭ，　６０１　ＣＰＵ，　６０２　ＲＯＭ，　６０３　ＲＡＭ，　６０８　通信部，　６４１　磁気ディスク，　６４２　光ディスク，　６４３　光磁気ディスク，　６４４　半導体メモリ，　６５１　ＣＰＵ，　６５２　ＲＯＭ，　６５３　ＲＡＭ，　６６３　通信部，　６８１　磁気ディスク，　６８２　光ディスク，　６８３　光磁気ディスク，　６８４　半導体メモリ

【書類名】図面

【図１】

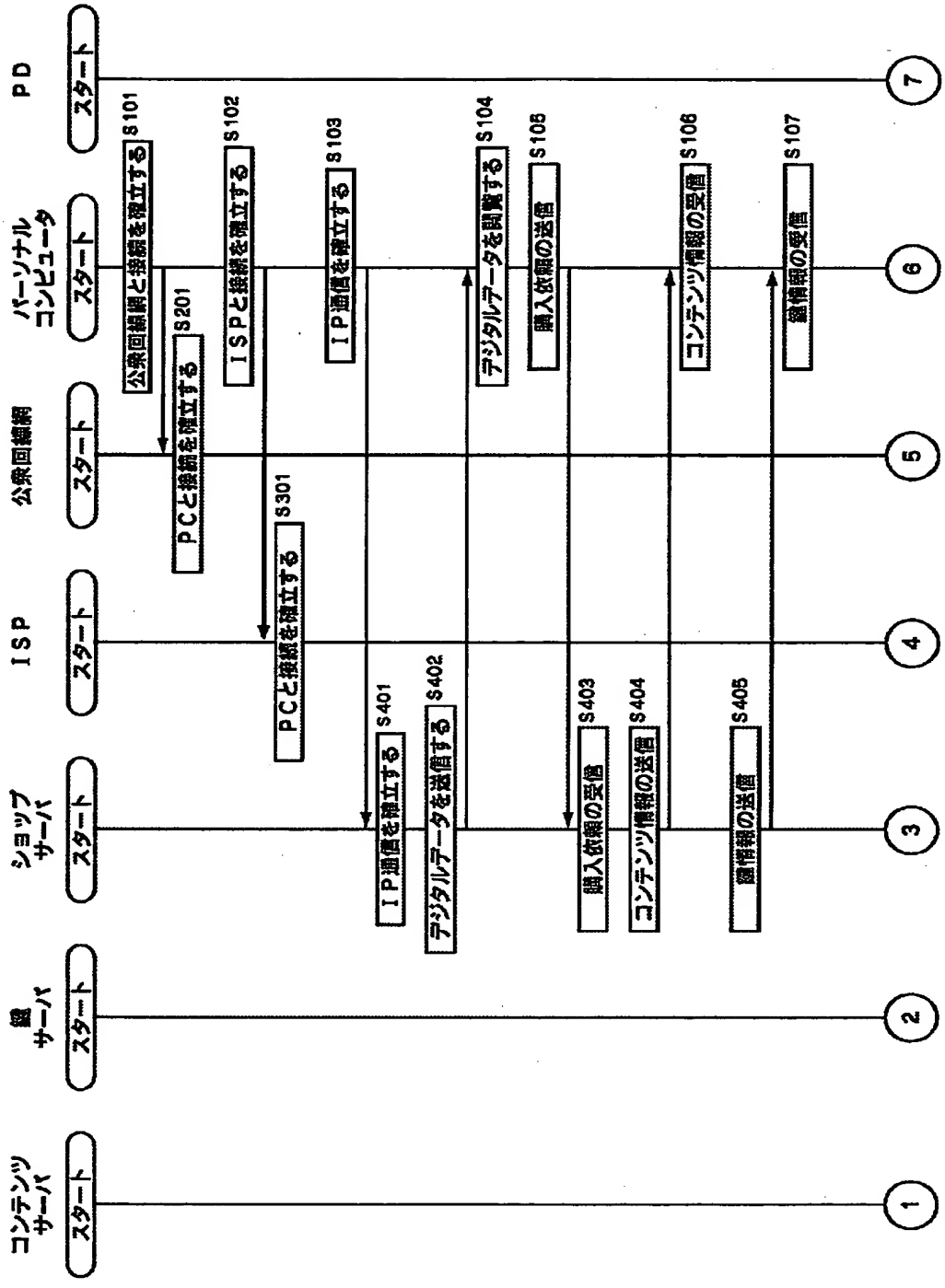

3
PM
2
PD
11
1
パーソナル
コンピュータ
表示操作指示
プログラム
LCM
12
4
通信ネットワーク
21
22
23
5
サーバ
鍵サーバ
コンテンツサーバ
ショップサーバ

【図２】


パーソナルコンピュータ
表示操作指示プログラム
LCM
利用条件管理プログラム
CDリッピングプログラム
コンバータプログラム
PD認証プログラム
ライセンス管理プログラム
サーバ制御プログラム
受信プログラム
鍵管理プログラム
受信プログラム
コンテンツ管理プログラム
鍵情報受信プログラム
コンテンツ情報受信プログラム
HTTP
Wap
IP通信プログラム
ISP接続プログラム
PHS／IMT通信プログラム
USB
PD
ライセンス管理プログラム
利用条件管理プログラム
PC認証プログラム
PM認証プログラム
鍵管理プログラム
コンテンツ管理プログラム
PM
ライセンス管理プログラム
PD認証プログラム
鍵管理プログラム
コンテンツ管理プログラム
公衆回線網
ISP
通信ネットワーク
ショップサーバ
鍵情報送信プログラム
コンテンツ情報送信プログラム
視聴プログラム
検索プログラム
閲覧プログラム
HTTP
Wap
IP通信プログラム
鍵サーバ
認証プログラム
鍵配信プログラム
鍵保存プログラム
鍵生成プログラム
HTTP
Wap
IP通信プログラム
コンテンツサーバ
コンテンツ保存プログラム
コンテンツ配信プログラム
HTTP
Wap
IP通信プログラム

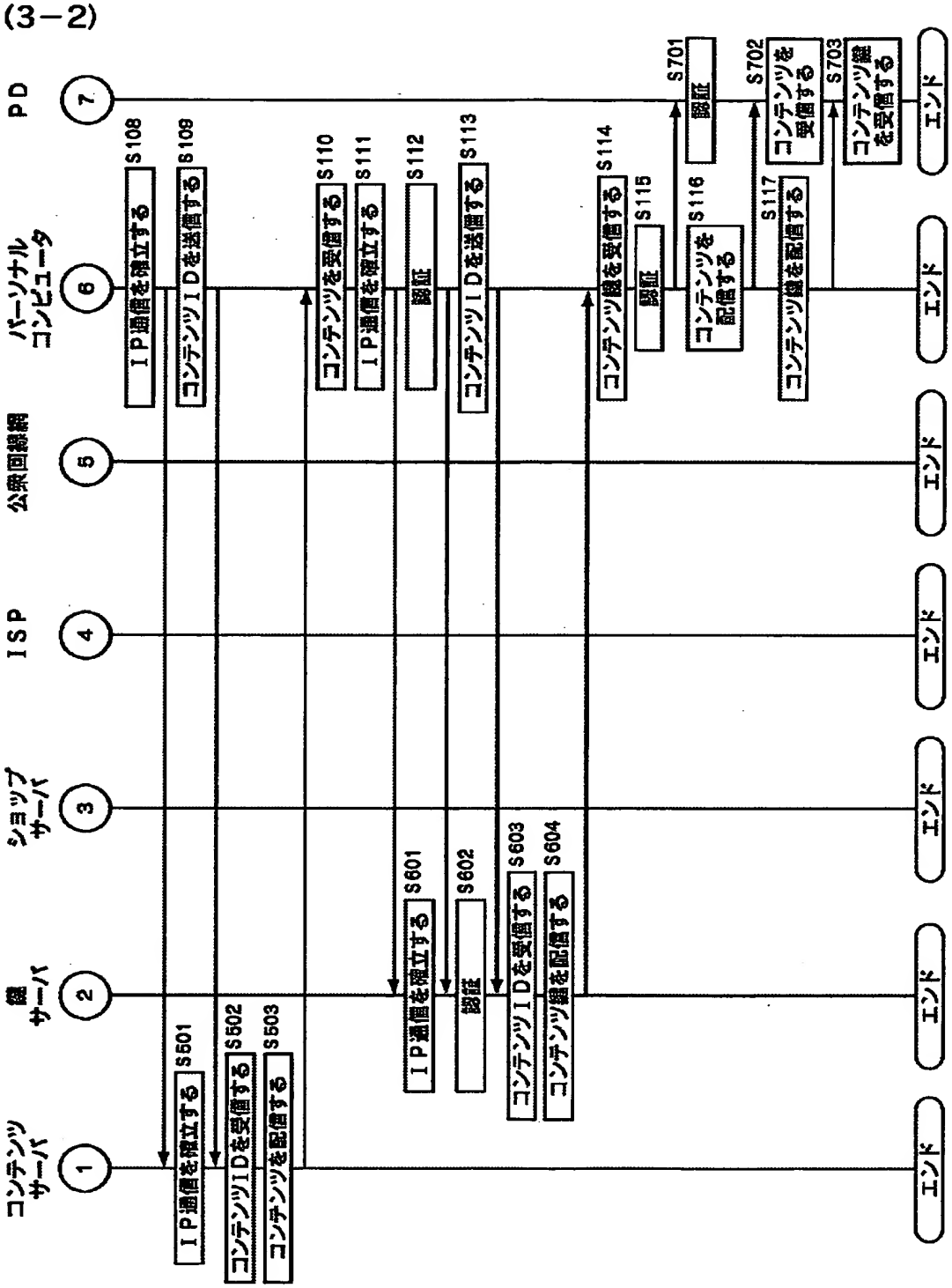
【図３】

(3－1)

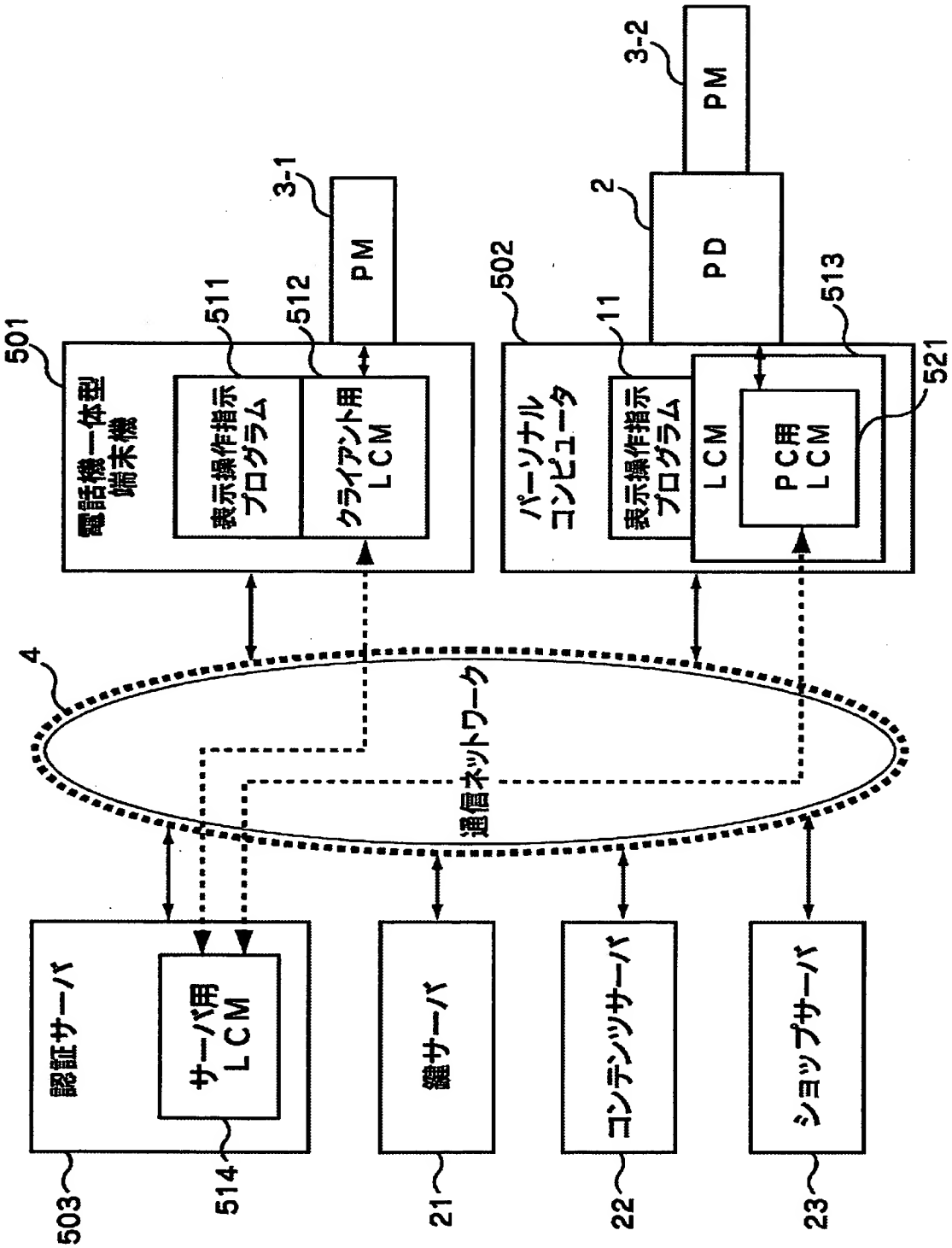

PD
パーソナルコンピュータ
公衆回線網
ISP
ショップサーバ
鍵サーバ
コンテンツサーバ
スタート
公衆回線と接続を確立する
S101
PCと接続を確立する
S201
ISPと接続を確立する
S102
PCと接続を確立する
S301
IP通信を確立する
S103
IP通信を確立する
S401
デジタルデータを送信する
S402
デジタルデータを閲覧する
S104
購入依頼の送信
S105
購入依頼の受信
S403
コンテンツ情報の送信
S404
コンテンツ情報の受信
S106
鍵情報の送信
S405
鍵情報の受信
S107
1
2
3
4
5
6
7

【図４】

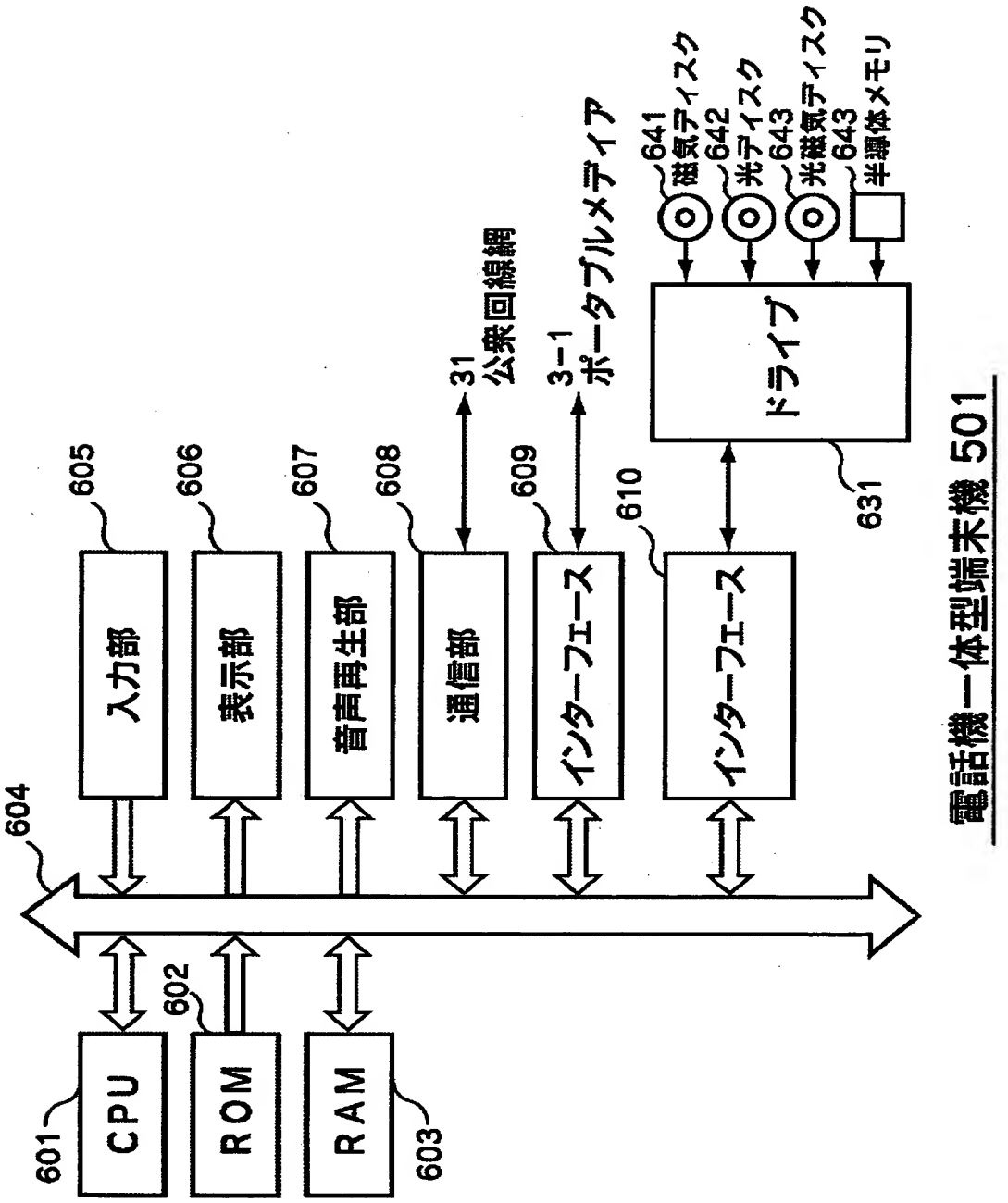
(3－2)


コンテンツサーバ
鍵サーバ
ショップサーバ
ISP
公衆回線網
パーソナルコンピュータ
PD
エンド
IP通信を確立する
コンテンツIDを送信する
コンテンツを受信する
認証
コンテンツIDを受信する
コンテンツを配信する
コンテンツ鍵を受信する
コンテンツを配信する
コンテンツ鍵を配信する
コンテンツ鍵を受信する
S108
S109
S110
S111
S112
S113
S114
S115
S116
S117
S601
S602
S603
S604
S701
S702
S703

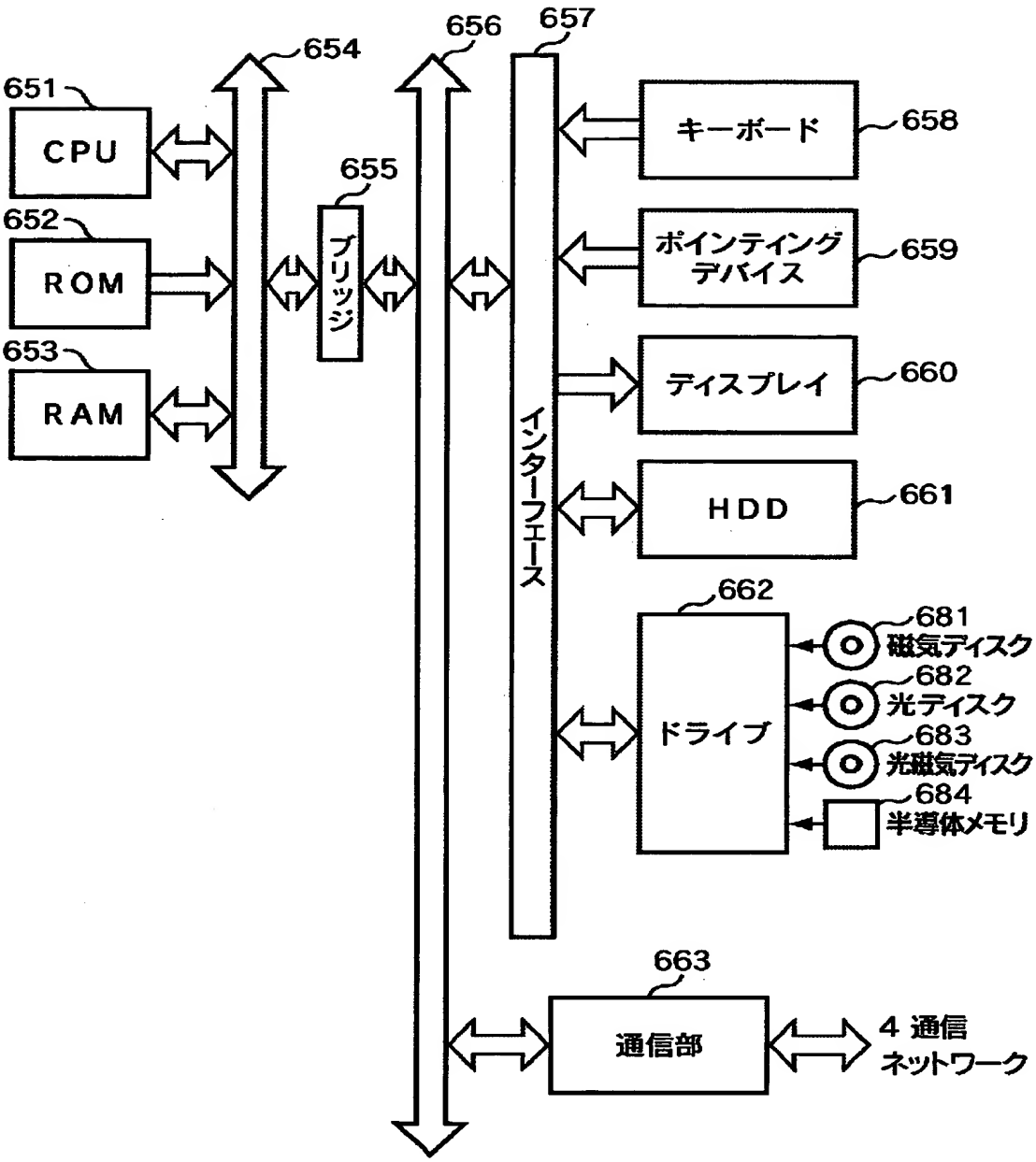
【図５】


501
電話機一体型端末機
511
表示操作指示プログラム
512
クライアント用LCM
3-1
PM
502
パーソナルコンピュータ
11
表示操作指示プログラム
2
PD
513
LCM
PC用LCM
521
3-2
PM
4
通信ネットワーク
認証サーバ
サーバ用LCM
503
514
鍵サーバ
21
コンテンツサーバ
22
ショップサーバ
23

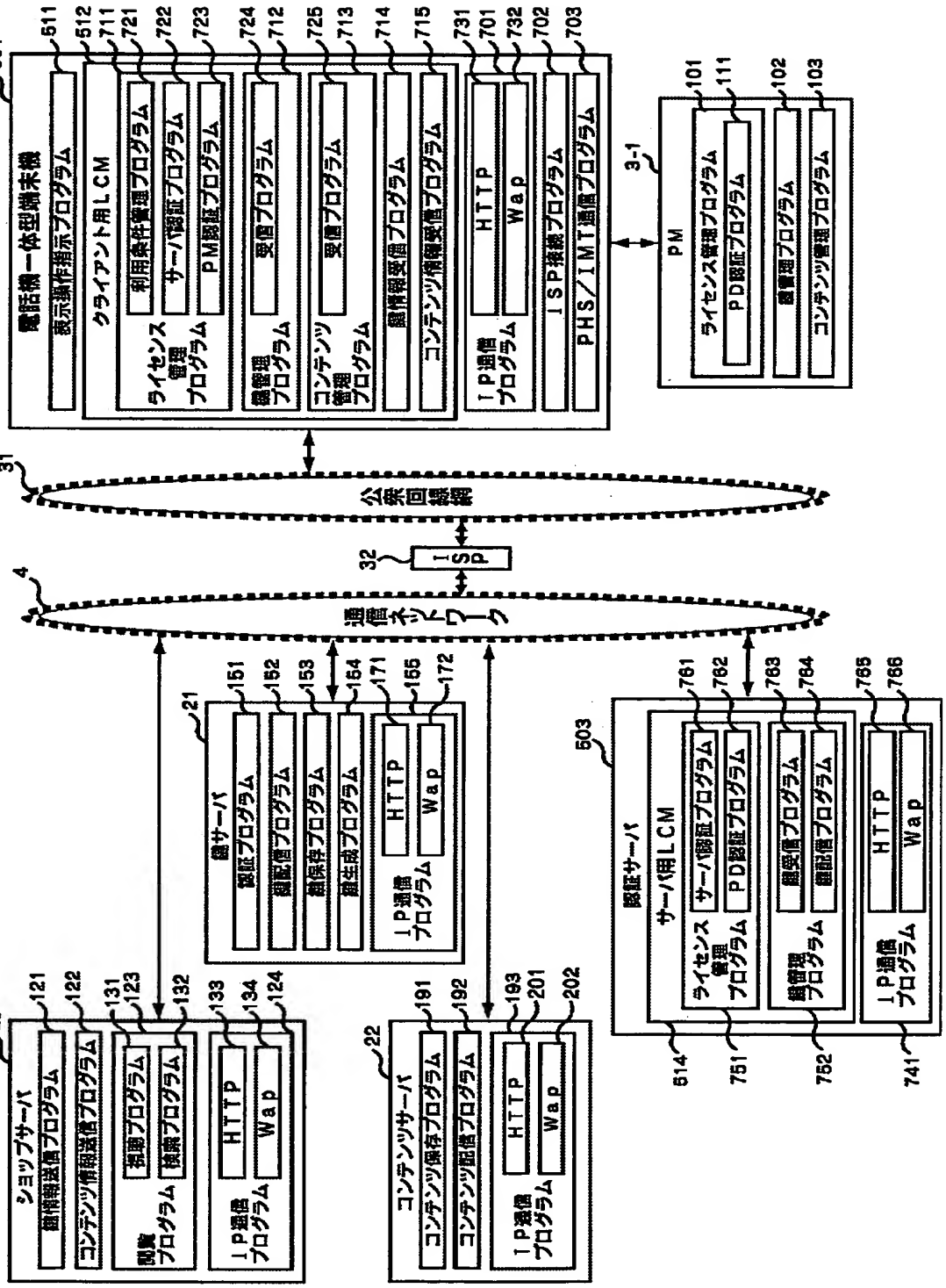
【図６】


電話機一体型端末機 501
604
605
入力部
606
表示部
607
音声再生部
608
通信部
609
インターフェース
610
インターフェース
631
ドライブ
641
磁気ディスク
642
光ディスク
643
光磁気ディスク
643
半導体メモリ
3-1
ポータブルメディア
31
公衆回線網
601
CPU
602
ROM
603
RAM

【図７】

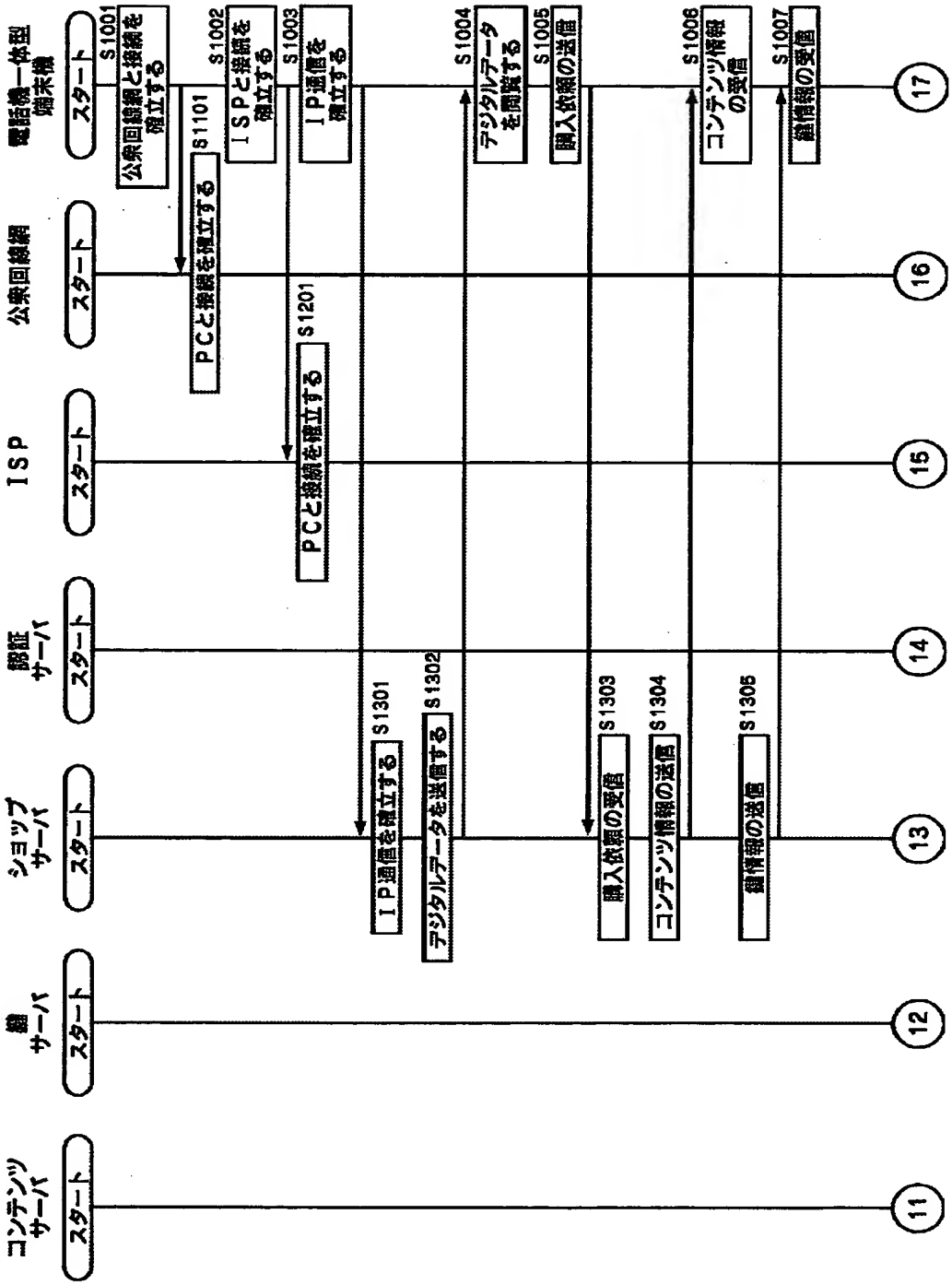

651
CPU
652
ROM
653
RAM
654
655
ブリッジ
656
657
インターフェース
キーボード
658
ポインティングデバイス
659
ディスプレイ
660
HDD
661
662
ドライブ
681
磁気ディスク
682
光ディスク
683
光磁気ディスク
684
半導体メモリ
663
通信部
4 通信ネットワーク
認証サーバ503

【図８】


501
511
512
711
721
722
723
724
712
725
713
714
715
731
701
732
702
703
電話機一体型端末機
表示操作指示プログラム
クライアント用ＬＣＭ
利用条件管理プログラム
サーバ認証プログラム
ＰＭ認証プログラム
ライセンス管理プログラム
受信プログラム
課金管理プログラム
受信プログラム
コンテンツ管理プログラム
履歴情報受信プログラム
コンテンツ情報受信プログラム
ＨＴＴＰ
Ｗａｐ
ＩＰ通信プログラム
ＩＳＰ接続プログラム
ＰＨＳ／ＩＭＴ通信プログラム
3-1
101
111
102
103
ＰＭ
ライセンス管理プログラム
ＰＤ認証プログラム
課金管理プログラム
コンテンツ管理プログラム
31
公衆回線網
32
ＩＳＰ
4
通信ネットワーク
21
151
152
153
154
171
155
172
蓄サーバ
認証プログラム
履配信プログラム
履保存プログラム
履生成プログラム
ＩＰ通信プログラム
ＨＴＴＰ
Ｗａｐ
503
761
762
763
784
765
766
認証サーバ
サーバ用ＬＣＭ
ライセンス管理プログラム
サーバ認証プログラム
ＰＤ認証プログラム
課金管理プログラム
履受信プログラム
履配信プログラム
ＩＰ通信プログラム
ＨＴＴＰ
Ｗａｐ
614
751
762
741
23
121
122
131
123
132
133
134
124
ショップサーバ
履情報送信プログラム
コンテンツ情報送信プログラム
閲覧プログラム
視聴プログラム
検索プログラム
ＩＰ通信プログラム
ＨＴＴＰ
Ｗａｐ
22
191
192
193
201
202
コンテンツサーバ
コンテンツ保存プログラム
コンテンツ配信プログラム
ＩＰ通信プログラム
ＨＴＴＰ
Ｗａｐ

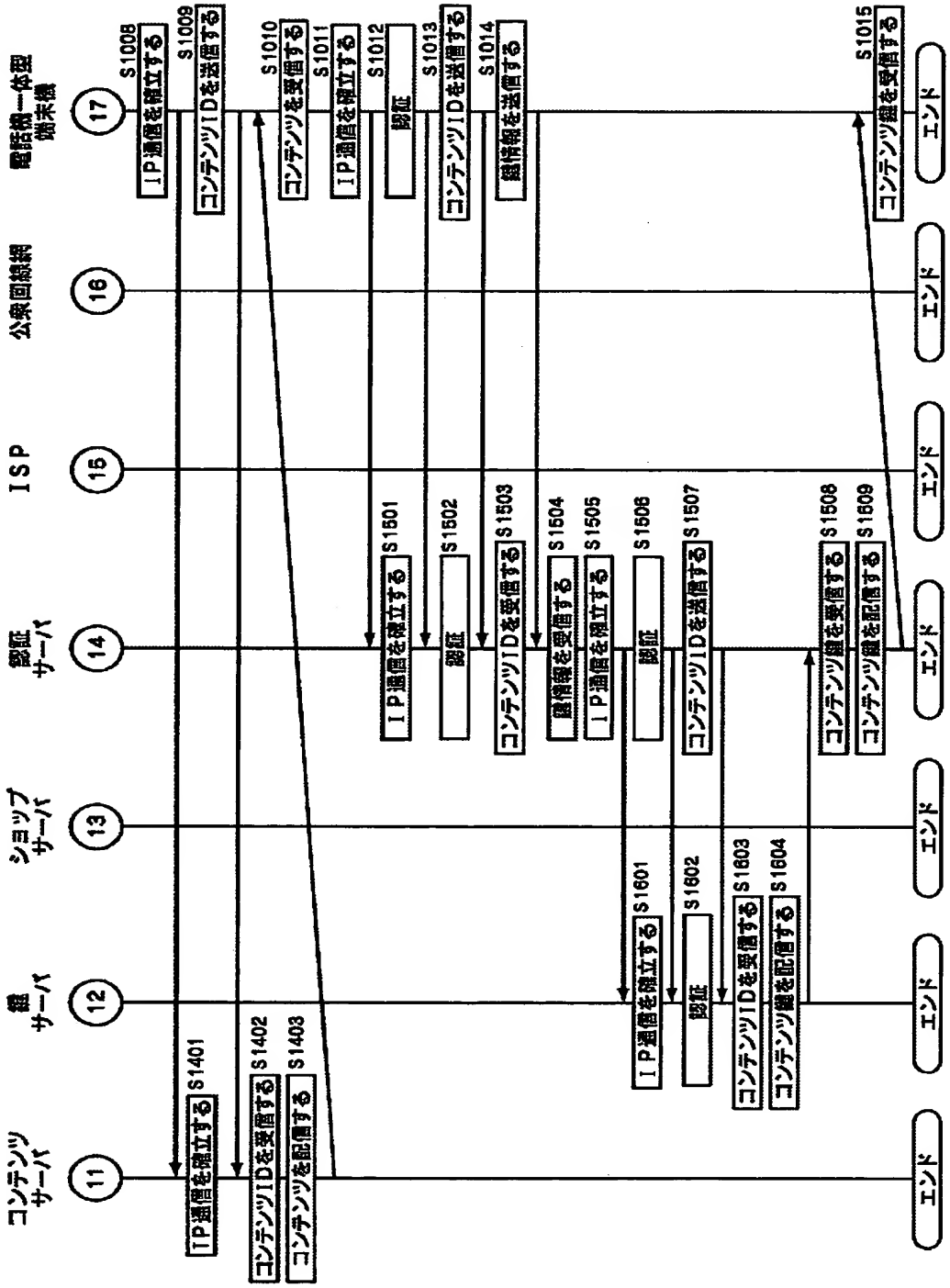
【図９】

(9－1)


電話機一体型端末機
公衆回線網
ISP
認証サーバ
ショップサーバ
銀サーバ
コンテンツサーバ
スタート
S1001
公衆回線網と接続を確立する
S1002
ISPと接続を確立する
S1003
IP通信を確立する
S1004
デジタルデータを同期する
S1005
購入依頼の送信
S1006
コンテンツ情報の受信
S1007
銀情報の受信
S1101
PCと接続を確立する
S1201
PCと接続を確立する
S1301
IP通信を確立する
S1302
デジタルデータを送信する
S1303
購入依頼の受信
S1304
コンテンツ情報の送信
S1305
銀情報の送信
17
16
15
14
13
12
11

【図１０】

(9－2)


コンテンツサーバ
⑪
認サーバ
⑫
ショップサーバ
⑬
認証サーバ
⑭
ISP
⑮
公衆回線網
⑯
電話機一体型端末機
⑰
S1008 IP通信を確立する
S1009 コンテンツIDを送信する
S1010 コンテンツを受信する
S1011 IP通信を確立する
S1012 認証
S1013 コンテンツIDを送信する
S1014 個情報を送信する
S1015 コンテンツ鍵を受信する
エンド
S1401 IP通信を確立する
S1402 コンテンツIDを受信する
S1403 コンテンツを配信する
S1501 IP通信を確立する
S1502 認証
S1503 コンテンツIDを受信する
S1504 個情報を受信する
S1505 IP通信を確立する
S1506 認証
S1507 コンテンツIDを送信する
S1508 コンテンツ鍵を受信する
S1509 コンテンツ鍵を配信する
S1601 IP通信を確立する
S1602 認証
S1603 コンテンツIDを受信する
S1604 コンテンツ鍵を配信する

【書類名】　　要約書

【要約】

【課題】　不正なコンテンツの利用を防止しつつ、迅速に、コンテンツをダウンロードする。

【解決手段】　PD認証プログラム７６２は、電話機一体型端末機５０１を認証する。サーバ認証プログラム７６１は、鍵サーバ２１を認証する。サーバ用ＬＣＭ５１４は、電話機一体型端末機５０１からの、鍵サーバ２１を特定するデータおよび鍵の要求の受信を制御する。サーバ用ＬＣＭ５１４は、鍵サーバ２１を特定するデータに基づき、鍵サーバ２１に鍵の要求を送信するとともに、鍵サーバ２１から鍵を受信するように通信を制御する。鍵配信プログラム７６４は、電話機一体型端末機５０１への鍵の送信を制御する。

【選択図】　　図８

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社